SPECYFIKACJA

ISTOTNYCH WARUNKÓW ZAMÓWIENIA

dla zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego o wartości mniejszej niż kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Prawo zamówień publicznych pod nazwą:

„Dostawa aktualizacji oprogramowania antywirusowego na potrzeby WUP”

ZNAK SPRAWY: WUP.XVA.322.265.MBi.2019

Ogłoszenie o zamówieniu zostało zamieszczone w Biuletynie Zamówień Publicznych w dniu 15 listopada 2019 r. pod nr 621745-N–2019 oraz na tablicy ogłoszeń w miejscu publicznie dostępnym w siedzibie Zamawiającego i na stronie internetowej: www.wup.pl

Podstawa prawna:

Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych
(tekst jednolity Dz. U. z 2019 r. poz. 1843)
oraz akty wykonawcze do tej ustawy

Szczecin, 2019 r.

I. Nazwa oraz adres Zamawiającego.

1. Województwo Zachodniopomorskie – Wojewódzki Urząd Pracy, 70-383 Szczecin, ul. A. Mickiewicza 41, tel.: 91/ 42-56-100, fax.: 91/ 42-56-103.
2. Godziny pracy Urzędu: 7:30- 15:30 od poniedziałku do piątku.
3. Adres strony internetowej: www.wup.pl.
4. Adres e-mail: przetargi@wup.pl.
5. Numer konta bankowego**: 56 1020 4795 0000 9102 0264 7832.**
6. **NIP: 851-26-80-829**
7. Znak postępowania **WUP.XVA.322.265.MBi.2019**

UWAGA: w korespondencji kierowanej do Zamawiającego należy posługiwać się tym znakiem.

II. Tryb udzielenia zamówienia.

1. Niniejsze postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie art. 39 i nast. ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych zwanej dalej „ustawą PZP".
2. W zakresie nieuregulowanym niniejszą Specyfikacją Istotnych Warunków Zamówienia, zwaną dalej „SIWZ", zastosowanie mają przepisy ustawy PZP.
3. Wartość zamówienia **nie przekracza** równowartości kwoty określonej w przepisach wykonawczych wydanych n a podstawie art. 11 ust. 8 ustawy PZP.
4. **UWAGA! W niniejszym postępowaniu mają zastosowanie przepisy art. 24 aa ustawy Pzp, tj.** Zamawiający **najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu**.
5. **Jeżeli wykonawca, o którym mowa w pkt.** 4 uchyla się od zawarcia umowy, lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, zamawiający może zbadać, czy nie podlega wykluczeniu oraz czy spełnia warunki udziału w postępowaniu wykonawca, który złożył ofertę najwyżej ocenianą spośród pozostałych ofert.
6. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej „RODO") informujemy, że:
7. Administratorem danych osobowych w zakresie przedmiotowej umowy jest Wojewódzki Urząd Pracy w Szczecinie, mający siedzibę przy ul. Mickiewicza 41, 70-383 Szczecin. Z administratorem danych można się skontaktować poprzez adres e-mail: sekretariat@wup.pl lub telefonicznie pod numerem 91/42-56-102 lub pisemnie na adres siedziby administratora.

8. Z administratorem danych można się skontaktować poprzez adres e-mail: sekretariat@wup.pl lub telefonicznie pod numerem 91/42-56-102 lub pisemnie na adres siedziby administratora.
9. Z Inspektorem ochrony danych osobowych w Wojewódzkim Urzędzie Pracy w można się skontaktować poprzez adresem e-mail: iod@wup.pl lub pisemnie składając wniosek na adres siedziby Urzędu, o którym mowa w ust. 7.
10. Dane osobowe zgromadzone w ramach przedmiotowej umowy przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu realizacji przedmiotowej umowy.
11. Odbiorcami zgromadzonych danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w tym przedmiotowa umowa. Dane mogą być przekazane także kurierom oraz podmiotom świadczącym usługi pocztowe oraz na stronie Biuletynu Informacji Publicznej Urzędu.
12. Dane osobowe będą przechowywane przez okres wynikający z Jednolitego Rzeczowego Wykazu Akt obowiązującego u Zamawiającego.
13. Obowiązek podania przez Wykonawcę danych osobowych dotyczących bezpośrednio gromadzonych danych osobowych jest wymogiem, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego oraz realizacją przedmiotowej umowy.
14. W odniesieniu do zgromadzonych danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
    a) na podstawie art. 15 RODO, osoba której dane dotyczą posiada prawo dostępu do swoich danych osobowych,
    b) na podstawie art. 16 RODO, osoba której dane dotyczą posiada prawo do sprostowania swoich danych osobowych,
    c) na podstawie art. 18 RODO, osoba której dane dotyczą posiada prawo do żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO,
    d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych danej osoby narusza przepisy RODO.

13. W odniesieniu do zgromadzonych danych osobowych, osobie której dane dotyczą, nie przysługuje:
    a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
    b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
    c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania zgromadzonych danych osobowych jest art. 6 ust. 1 lit. c RODO.
14. Gromadzone dane są odpowiednio zabezpieczone oraz chronione z zastosowaniem środków technicznych i organizacyjnych, aby dane zgromadzone nie były zmieniane przez osoby nieupoważnione lub nie były udostępniane osobom nieupoważnionym.

III. Opis przedmiotu zamówienia.

1. Przedmiotem zamówienia jest „Dostawa zestawów komputerowych wraz z oprogramowaniem”.
2. Szczegółowy opis przedmiotu zamówienia stanowi **Załącznik nr 1** do SIWZ.
3. Wykonawca zobowiązany jest zrealizować zamówienie na zasadach i warunkach opisanych w projekcie umowy stanowiącym **Załącznik nr 4** do SIWZ.
4. Wspólny Słownik Zamówień CPV:
    - 48761000-0 Pakiety oprogramowania antywirusowego
5. Zamawiający **nie dopuszcza** możliwości składania ofert częściowych w rozumieniu art. 2 pkt 6 ustawy Pzp.
6. Zamawiający **nie dopuszcza** możliwości składania ofert wariantowych.
7. Zamawiający nie przewiduje zawarcia umowy ramowej.
8. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.
9. Zamawiający zamierza przeznaczyć na realizację zamówienia **kwotę w wysokości: 27 000,00 zł brutto.**
10. Zamawiający **nie przewiduje** możliwości udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt 7.
11. Zamawiający **nie zastrzega** obowiązku osobistego wykonania przez wykonawcę następujących prac związanych **z rozmieszczeniem i instalacją przedmiotu dostawy.**

IV. Termin wykonania zamówienia.

Zamawiający wymaga realizacji zamówienia w terminie **do 14 dni kalendarzowych od dnia zawarcia umowy.** Dokładny termin realizacji przedmiotu zamówienia, jako kryterium oceny wykonania przedmiotu zamówienia, Wykonawca wskaże w formularzu oferty cenowej.

V. Warunki udziału w postępowaniu.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
    1) nie podlegają wykluczeniu na podstawie art. 24 ust. 1 pkt 12-23 i 24 ust. 5 pkt 1 ustawy Pzp
    2) Zamawiający nie określa warunków udziału w postępowaniu.

Va Podstawy wykluczenia, o których mowa w art. 24 ust 1 pkt 12-23 ustawy Pzp.

W przedmiotowym postępowaniu Zamawiający zgodnie z art. 24 ust. 1 pkt 12-23 ustawy Pzp wykluczy:

1. Wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie został zaproszony do negocjacji lub złożenia ofert wstępnych albo ofert, lub nie wykazał braku podstaw wykluczenia;
2. Wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
   1) o którym mowa w art. 165a, art. 181-188, art. 189a, art. 218-221, art. 228-230a, art. 250a, art. 258 lub art. 270-309 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (t .j. Dz. U. z 2018 r. poz. 1600, z późn. zm.) lub art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (t. j. Dz. U. z 2018 poz. 1263 z późn. zm.).
   2) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny,
   3) skarbowe,
   4) o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. 2012 poz. 769);
3. Wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 2 niniejszego rozdziału SIWZ;
4. Wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
5. Wykonawcę, który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawieniu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub obiektywne i niedyskryminacyjne kryteria, zwane dalej "kryteriami selekcji", lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów;
6. Wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia;
7. Wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
8. Wykonawcę, który brał udział w przygotowaniu postępowania o udzielenie zamówienia lub którego pracownik, a także osoba wykonująca pracę na podstawie umowy zlecenia, o dzieło, agencyjnej lub innej umowy o świadczenie usług, brał udział w przygotowaniu takiego postępowania, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;

9. Wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;
10. Wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t. j. Dz. U. z 2019 r. poz. 628 z późn. zm.);
11. Wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne;
12. Wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t. j. Dz. U. z 2019 r. poz. 369 z późn. zm.), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że istniejące między nimi powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.
13. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16-20 lub ust. 5 pkt. 1 (Rozdział V.b. SIWZ), może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu wykonawcy. Przepisu zdania pierwszego nie stosuje się, jeżeli wobec wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.
14. Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu wykonawcy, uzna za wystarczające dowody przedstawione na podstawie art. 24 ust. 8 ustawy Pzp.
15. W przypadkach, o których mowa w art. 24 ust. 1 pkt 19, przed wykluczeniem wykonawcy, zamawiający zapewnia temu wykonawcy możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji. Zamawiający wskazuje w protokole sposób zapewnienia konkurencji.
16. Wykluczenie Wykonawcy następuje zgodnie z art. 24 ust. 7 ustawy Pzp.
17. Zamawiający może wykluczyć wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

Vb Podstawy wykluczenia, o których mowa w art. 24 ust. 5 pkt 1 ustawy PZP.

Dodatkowo Zamawiający przewiduje wykluczenie wykonawcy:

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

likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (t. j. Dz. U. z 2019 r. poz. 243 z późn. zm.) lub którego upadłość ogłoszono, z wyjątkiem wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (t. j. Dz. U. z 2019 r. poz. 498 z późn. zm.).

VI. Wykaz oświadczeń lub dokumentów, potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

1. **Wraz z ofertą każdy Wykonawca musi dołączyć aktualne na dzień składania ofert oświadczenia w zakresie wskazanym w Załączniku nr 3 do SIWZ.** Informacje zawarte w oświadczeniach będą stanowić wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu Oświadczenia i ofertę Wykonawca zobowiązany jest złożyć w formie pisemnej.
2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców (np. konsorcjum; wspólnicy spółki cywilnej są traktowani jak Wykonawcy składający ofertę wspólną) oświadczenia, w tym Załącznik nr 3 do SIWZ, składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia te mają potwierdzać spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje, brak podstaw do wykluczenia.
3. Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu, zamieszcza informacje o podwykonawcach w oświadczeniu, zgodnie z Załącznikiem nr 3 do SIWZ wypełniając pkt 2.
4. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
5. W przypadku powierzenia realizacji zamówienia podwykonawcom Wykonawca w pkt D Załącznika nr 2 do SIWZ (Formularz ofertowy), zobowiązany jest do wskazania części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez wykonawcę firm podwykonawców. Brak takiego oświadczenia wskazywać będzie, że Wykonawca przedmiot zamówienia zrealizuje bez udziału podwykonawców.
6. Jeżeli zamawiający stwierdzi, że wobec danego podwykonawcy zachodzą podstawy wykluczenia, Wykonawca obowiązany jest zastąpić tego podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia podwykonawcy.
7. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
8. **Zamawiający przed udzieleniem zamówienia, może wezwać Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów:**

1) **Odpis** z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy Pzp; W przypadku wskazania dostępności przedmiotowych dokumentów w formie elektronicznej pod określonym adresem internetowym ogólnodostępnych i bezpłatnych baz danych, Zamawiający pobiera samodzielnie z tych baz danych wskazane przez Wykonawcę dokumenty. W celu potwierdzenia braku podstaw wykluczenia, o którym mowa w Rozdziale Vb SIWZ.

   W przypadku wykonawców składających ofertę wspólną w/w dokument składa każdy z wykonawców składających ofertę wspólną. Dokument ten należy złożyć w oryginale lub kopii potwierdzonej za zgodność z oryginałem.

   a) Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu o którym mowa w pkt 8 ppkt 1, składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości lub wskazać dostępność przedmiotowych dokumentów w formie elektronicznej pod określonym adresem internetowym ogólnodostępnych i bezpłatnych baz danych, z których Zamawiający w formie elektronicznej samodzielnie pobierze wskazane przez Wykonawcę dokumenty. Zamawiający wymaga, aby w sytuacji, gdy przedmiotowe dokumenty będą dostępne pod wskazanym przez Wykonawcę adresem internetowym wyłączenie w języku obcym (innym niż język polski), Zamawiający żąda ich złożenia w formie pisemnej wraz tłumaczeniem na język polski.
   b) Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w pkt 9 ppkt 1, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby.
   c) Dokumenty o których mowa pkt 8 ppkt 1 litera a) i b) niniejszego rozdziału, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
   d) W zakresie dokumentów, o których mowa w pkt 8 ppkt 1) niniejszego rozdziału, albo odpowiadających im dokumentów określonych w pkt 8 ppkt 1 litera a) i b) – w przypadku wskazania przez Wykonawcę oświadczeń lub dokumentów, które znajdują się w posiadaniu Zamawiającego, w szczególności oświadczeń lub dokumentów przechowywanych przez Zamawiającego zgodnie z art. 97 ust. 1 ustawy Pzp, Zamawiający w celu potwierdzenia braku podstaw do wykluczenia (art. 25 ust. 1 pkt 3 ustawy Pzp), korzysta z posiadanych oświadczeń lub dokumentów o ile są one aktualne.
   e) W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę, Zamawiający może zwrócić się do właściwych organów odpowiednio kraju, w którym

Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

2) Wykonawca, w terminie 3 dni, od dnia zamieszczenia na stronie internetowej, tj. https://www.wup.pl/pl/urzad/zamowienia/zamowienia-publiczne/ informacji, o której mowa art. 86 ust. 5 ustawy Pzp, przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp, zgodnie ze wzorem stanowiącym Załącznik nr 5 do niniejszej SIWZ. **W przypadku składania oferty wspólnej w/w oświadczenie składa każdy z wykonawców składających ofertę wspólną. Dokument ten należy złożyć w oryginale.**

9. *W zakresie nieuregulowanym SIWZ, zastosowania maja przepisy rozporządzenia Prezesa Rady Ministrów z dnia 27 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia.*
10. Jeżeli wykonawca nie złoży oświadczenia, o którym mowa w rozdz. VI. 1. niniejszej SIWZ, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy PZP, **lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez zamawiającego wątpliwości, zamawiający wzywa do ich złożenia, uzupełnienia lub poprawienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.**
11. Oświadczenia, o których mowa w rozporządzeniu dotyczące Wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega Wykonawca na zasadach określonych w art. 22 a ustawy Pzp, składane są w oryginale.
12. Dokumenty, o których mowa w SIWZ, inne niż oświadczenia, o których mowa w pkt 1 niniejszego rozdziału SIWZ, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem.
13. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.
14. Poświadczenie za zgodność z oryginałem następuje w formie pisemnej podpisane własnoręcznym podpisem. Poświadczenie za zgodność z oryginałem dokonywane w formie pisemnej powinno być sporządzone w sposób umożliwiający identyfikacje podpisu (np. wraz z imienną pieczęcią osoby poświadczającej kopie dokumentu za zgodność z oryginałem).
15. W przypadku gdy o udzielenie zamówienia ubiega się kilku Wykonawców (konsorcjum, wspólnicy spółki cywilnej) do oferty winni załączyć dokument pełnomocnictwa wystawionego zgodnie z art. 23 ust. 2 ustawy Pzp, tj. o zakresie co najmniej: do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego, ewentualnie umowę o współdziałaniu, z której będzie wynikać przedmiotowe pełnomocnictwo.

16. Jeżeli z przedstawionych dokumentów wynika, że osoba, która podpisała ofertę nie jest uprawiona do reprezentacji Wykonawcy w obrocie gospodarczym, do oferty załączyć należy dokument pełnomocnictwa. W przypadku złożenia kopii pełnomocnictwa musi być ono potwierdzone za zgodność z oryginałem przez notariusza.
17. Zamawiający zastrzega sobie prawo żądania przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentu, innych niż oświadczenia, gdy złożona przez Wykonawcę kopia dokumentu będzie nieczytelna lub będzie budzić wątpliwości co do jej prawdziwości.
18. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim. Dokumenty lub oświadczenia sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski. W toku prowadzonego postępowania wszelkie wyjaśnienia, oświadczenia, wnioski, zawiadomienia, informacje itp. składane są zgodnie z powyższym.

VII. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów

1. W postępowaniu komunikacja między Zamawiającym a Wykonawcami odbywa się za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2018 r. poz. 2188 z późn. zm.), osobiście za pośrednictwem posłańca, przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2019 r. poz. 123), lub faksu z uwzględnieniem wymogów dotyczących formy, ustanowionych poniżej w pkt 2-5 niniejszego rozdziału.
2. Wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje Zamawiający oraz Wykonawcy mogą przekazywać pisemnie, faksem lub drogą elektroniczną, za wyjątkiem oferty, umowy, oraz oświadczeń i dokumentów wymienionych w rozdziale VI niniejszej SIWZ (dotyczy także ich złożenia w wyniku wezwania o którym mowa w art. 26 ust. 3 i ust. 2 ustawy Pzp), dla których Prawodawca przewidział wyłącznie formę pisemną.
3. Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane przez Wykonawcę pisemnie, winny być składane na adres: Wojewódzki Urząd Pracy, ul. A. Mickiewicza 41, Kancelaria (na parterze, w holu głównym Urzędu), 70-383 Szczecin.
4. Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane przez Wykonawcę drogą elektroniczną na adres e mail: **przetargi@wup.pl** lub faksem na nr 91-42-56-103.
5. Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane za pomocą faksu lub w formie elektronicznej wymagają, na żądanie każdej ze stron, niezwłocznego potwierdzenia faktu ich otrzymania.
6. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SIWZ nie później niż do końca dnia, w którym upływa połowa terminu składania ofert. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, poprzez zamieszczenie ich na stronie internetowej (www.wup.pl w zakładce Urząd/Zamówienia/Zamówienia publiczne), na której zamieszczona została niniejsza SIWZ, 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. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynął po upływie terminu składania wniosku, o którym mowa powyżej lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień, albo pozostawić wniosek bez rozpoznania.
8. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SIWZ.
9. Zamawiający nie przewiduje zwołania zebrania Wykonawców w celu wyjaśnienia treści SIWZ.
10. W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.
11. Zamawiający informuje, że przepisy ustawy PZP nie pozwalają na jakikolwiek inny kontakt - zarówno z Zamawiającym jak i osobami uprawnionymi do porozumiewania się z Wykonawcami - niż wskazany w niniejszym rozdziale SIWZ. Oznacza to, że Zamawiający nie będzie reagował na inne formy kontaktowania się z nim, w szczególności na kontakt telefoniczny lub/i osobisty w swojej siedzibie.

VIII. Wymagania dotyczące wadium.

Zamawiający nie **wymaga wniesienia** wadium.

IX. Termin związania ofertą.

1. Wykonawca będzie związany ofertą przez okres **30 dni**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert. (art. 85 ust. 5 ustawy PZP).
2. Wykonawca może przedłużyć termin związania ofertą, na czas niezbędny do zawarcia umowy, samodzielnie lub na wniosek Zamawiającego, z tym, że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres nie dłuższy jednak niż 60 dni.
3. Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą skutkuje odrzuceniem oferty.
4. Zgoda Wykonawcy na przedłużenie terminu związania ofertą winna być wyrażona na piśmie.

X. Opis sposobu przygotowywania ofert.

1. Wykonawca, w myśl art. 25 a ustawy Pzp, zobowiązany jest do złożenia wyłącznie aktualnych na dzień składania ofert, następujących oświadczeń i dokumentów:
   1) **Załącznik nr 2-** Formularz ofertowy.

2) **Załącznik nr 3-** Oświadczenie z art. 25 a ust. 1 Pzp- wstępne potwierdzenie braku podstawy wykluczenia.

3) **Odpowiednie pełnomocnictwo** do reprezentowania Wykonawcy / wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia, ewentualnie umowa o współdziałaniu, z której wynikać będzie przedmiotowe pełnomocnictwo. Pełnomocnik może być ustanowiony do reprezentowania Wykonawców w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy. Pełnomocnictwo winno być załączone w formie oryginału lub notarialnie poświadczonej kopii.

2. Wykonawca musi być świadomy, że na podstawie ustawy z dnia 6.06.1997 r. – Kodeks karny wykonawcy (t. j. Dz. U. z 2018 r. poz. 1600 z późn. zm.) art. 297 §1: *„kto w celu uzyskania dla siebie lub kogo innego zamówienia publicznego, przedkłada podrobiony, poświadczający nieprawdę, albo nierzetelny dokument, albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania wymienionego zamówienia podlega karze pozbawienia wolności od 3 miesięcy do 5 lat".*
3. Oferta musi być napisana w języku polskim, na maszynie do pisania, komputerze lub inną trwałą i czytelną techniką oraz podpisana przez osobę(y) upoważnioną do reprezentowania Wykonawcy na zewnątrz i zaciągania zobowiązań w wysokości odpowiadającej cenie oferty.
4. W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę niewymienioną w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy, należy do oferty dołączyć stosowne pełnomocnictwo w oryginale lub kopii poświadczonej notarialnie.
5. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
6. Wykonawca ma prawo złożyć tylko jedną ofertę, zawierającą jedną, jednoznacznie opisaną propozycję. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
7. Treść złożonej oferty musi odpowiadać treści SIWZ.
8. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
9. Zaleca się, aby każda zapisana strona oferty była ponumerowana kolejnymi numerami, a cała oferta wraz z załącznikami była w trwały sposób ze sobą połączona (np. zbindowana, zszyta uniemożliwiając jej samoistną dekompletację), oraz zawierała spis treści.
10. Poprawki lub zmiany (również przy użyciu korektora) w ofercie, powinny być parafowane własnoręcznie przez osobę podpisującą ofertę.
11. Wykonawca nie może wprowadzić zmian do oferty ani wycofać jej po upływie terminu składania ofert.
12. Oferty złożone po terminie składania Zamawiający niezwłocznie zwraca wykonawcom.
13. Jeżeli termin składania ofert ulegnie przesunięciu, wówczas dokumenty, które do tego czasu utraciły swoją ważność powinny zostać uaktualnione w trybie wskazanym w pkt 19-20.
14. Ofertę należy złożyć w zamkniętej kopercie, w siedzibie Zamawiającego i oznakować w następujący sposób:

„Dostawa aktualizacji oprogramowania antywirusowego na potrzeby WUP"- WUP.XVA.322.265.MBi.2019"

Nie otwierać przed dniem 25 listopada 2019 r., godz. 12:00.

Na kopercie, oprócz opisu jw. należy umieścić nazwę i adres Wykonawcy.

15. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 ustawy Prawo zamówień publicznych oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca nie później niż w terminie składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu zastrzegł, że nie *mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.* ***Przez tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t. j. Dz. U. z 2018 poz. 419 z późn. zm.) rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działanie w celu zachowania ich poufności.***
16. W przypadku gdyby oferta zawierała informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji **Zamawiający zaleca**, aby informacje zastrzeżone jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnej wewnętrznej kopercie z oznakowaniem „tajemnica przedsiębiorstwa" lub spięte (zszyte) oddzielnie od pozostałych, jawnych elementów oferty w sposób niebudzący wątpliwości, które spośród zawartych w ofercie informacji stanowią taką tajemnicę. Strony zawierające informacje, o których mowa w zdaniu poprzednim, winny być oddzielnie ze sobą połączone, ale ponumerowane z zachowaniem kontynuacji numeracji stron oferty.
17. Zgodnie z art. 8 ust. 3 z związku z art. 86 ust. 4 ustawy Prawo zamówień publicznych Wykonawca nie może zastrzec informacji dotyczących ceny, nazwy (firmy) oraz adresu, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofercie.
18. Zamawiający informuje, że w przypadku kiedy wykonawca otrzyma od niego wezwanie w trybie art. 90 ustawy PZP, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa.
19. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty pod warunkiem, że Zamawiający otrzyma pisemne zawiadomienie o wprowadzeniu zmian przed terminem składania ofert. Powiadomienie o wprowadzeniu zmian musi być złożone wg takich samych zasad, jak składana oferta tj. w kopercie odpowiednio oznakowanej napisem „ZMIANA". Koperty oznaczone „ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy,

który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.

20. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie pisemnego powiadomienia, według tych samych zasad jak wprowadzanie zmian i poprawek z napisem na kopercie „WYCOFANIE". Koperty oznakowane w ten sposób będą otwierane w pierwszej kolejności po potwierdzeniu poprawności postępowania Wykonawcy oraz zgodności ze złożonymi ofertami. Koperty ofert wycofywanych nie będą otwierane.
21. Oferta, której treść nie będzie odpowiadać treści SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt 3 ustawy PZP zostanie odrzucona (art. 89 ust. 1 pkt 2 ustawy PZP). Wszelkie niejasności i wątpliwości dotyczące treści zapisów w SIWZ należy zatem wyjaśnić z Zamawiającym przed terminem składania ofert w trybie przewidzianym w rozdziale VII niniejszej SIWZ. Przepisy ustawy PZP nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów projektu umowy, po terminie otwarcia ofert.

XI. Miejsce i termin składania i otwarcia ofert.

1. Ofertę należy złożyć **w siedzibie Zamawiającego przy ul. A. Mickiewicza 41 w Szczecinie, Kancelaria Urzędu- hol główny na parterze, do dnia 25/11/2019 r., do godziny 12:00 i zaadresować zgodnie z opisem przedstawionym w rozdziale X SIWZ.**
2. Decydujące znaczenie dla oceny zachowania terminu składania ofert ma data i godzina wpływu oferty do Zamawiającego, a nie data jej wysłania przesyłką pocztową czy kurierską.
3. Oferta złożona po terminie wskazanym w rozdz. XI. 1 niniejszej SIWZ zostanie zwrócona wykonawcy zgodnie z zasadami określonymi w art. 84 ust. 2 ustawy PZP.
4. Otwarcie ofert nastąpi **w siedzibie Zamawiającego – pok. 38, w dniu 25/11/2019 r., o godzinie 12:30.**
5. Otwarcie ofert jest jawne.
6. Podczas otwarcia ofert Zamawiający odczyta informacje, o których mowa w art. 86 ust. 3 i 4 ustawy PZP.
7. Niezwłocznie po otwarciu ofert zamawiający zamieści na stronie https://www.wup.pl/pl/urzad/zamowienia/zamowienia-publiczne/ informacje dotyczące:
   a) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia;
   b) firm oraz adresów wykonawców, którzy złożyli oferty w terminie;
   c) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

XII. Opis sposobu obliczania ceny.

1) Wykonawca określa cenę realizacji zamówienia poprzez wskazanie w Formularzu ofertowym, sporządzonym wg wzoru stanowiącego **Załączniki nr 2** do SIWZ, łączną cenę umowną brutto oraz

termin realizacji przedmiotu zamówienia oraz informacje dotyczące Kryterium nr 3 (klauzule społeczne).

1. Łączna cena ofertowa brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia zgodnie z opisem przedmiotu zamówienia oraz projektem umowy określonym w niniejszej SIWZ.
2. Zamawiający **nie przewiduje** możliwości zmian ceny ofertowej brutto**.**
3. Ceny muszą być: podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
4. Cena oferty winna być wyrażona w złotych polskich (PLN).
5. Jeżeli w postępowaniu złożona będzie oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. W takim przypadku Wykonawca, składając ofertę, jest zobligowany poinformować zamawiającego, że wybór jego oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę **towarów**, których **dostawa** będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

XIII. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert.

1. Za ofertę najkorzystniejszą zostanie uznana oferta nie podlegająca odrzuceniu, zawierająca najkorzystniejszy bilans punktów w kryteriach:
   1) **„Łączna cena umowna brutto”- C;**
   2) **„Termin realizacji przedmiotu umowy”- T;**
   3) **„Klauzula społeczna”- K.**
2. Powyższym kryteriom Zamawiający przypisał następujące znaczenie:

Kryterium	Waga [%]	Liczba Punktów max	Sposób oceny wg wzoru
Łączna cena umowna brutto	**60 %**	**60**	$C = \frac{\text{Cena najtańszej oferty}}{\text{Cena badanej oferty}} \times 60 \text{ pkt}$
Termin realizacji przedmiotu umowy	**35 %**	**35**	• do 5 dni kalendarzowych – 35 pkt • od 6 do 10 dni kalendarzowych – 15 pkt • od 11 do 14 dni kalendarzowych – 0 pkt

Klauzula społeczna	**5 %**	**5**	• ZATRUDNIĘ nową osobę/ osoby z grup wskazanych do realizacji zamówienia - 5 punktów; • NIE ZATRUDNIĘ nowej osoby/ osób z grup wskazanych do realizacji zamówienia - 0 punktów.
RAZEM	**100%**	**100**	———————————————

3. **Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:**

   L = C + T + K

   gdzie:
   L – całkowita liczba punktów,
   C – punkty uzyskane w kryterium „Łączna cena umowna brutto",
   T – punkty uzyskane w kryterium „Termin realizacji przedmiotu umowy",
   K- punkty uzyskane w kryterium „Klauzula społeczna".

4. Ocena punktowa w kryterium nr 1 **„Łączna cena umowna brutto"** dokonana zostanie na podstawie łącznej ceny umownej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej. Maksymalna liczba punktów, która może zostać przyznana Wykonawcy w ocenie ww. kryterium wynosi 60 pkt**.**
5. Ocena punktowa w kryterium nr 2 **„Termin realizacji przedmiotu umowy"** dokonana zostanie na podstawie oświadczenia z zaoferowaną liczbą dni wskazaną przez Wykonawcę w ofercie. Oświadczenie w zakresie realizacji przedmiotu zamówienia składane jest poprzez wpisanie właściwej liczby dni, poprzez wypełnienie **pkt C ppkt 1) Załącznika nr 2 do** SIWZ (oferta cenowa). W przypadku nie wpisania żadnej wartości, wpisania mniej niż 1 dni, lub ułamków lub innej wartości niż pełne liczby od 1 do 14, Zamawiający uzna, że Wykonawca wykona przedmiot umowy w terminie maksymalnym tj. 14 dni kalendarzowych od dnia zawarcia umowy, a punktacja zostanie przyznana w oparciu o wartość 14 dni kalendarzowych. Maksymalna liczba punktów, która może zostać przyznana Wykonawcy w ocenie ww. kryterium wynosi 35 pkt.
6. Ocena punktowa w kryterium nr 3 **„Klauzula społeczna"** tj. **Zatrudnienie przy realizacji zamówienia nowych osób znajdujących się w trudnej sytuacji na rynku pracy „Klauzula społeczna",** dokonana zostanie na podstawie oświadczenia wskazanego przez Wykonawcę w ofercie cenowej. Oświadczenie w zakresie klauzuli społecznej przedmiotu zamówienia składane jest poprzez właściwe wskazanie/ wypełnienie w **pkt C ppkt 2) Załącznika nr 2 do** SIWZ (oferta cenowa).

   Niniejsze kryterium dotyczy liczby osób, którzy będą nowo zatrudnione przez Wykonawcę lub Podwykonawcę do realizacji przedmiotu zamówienia, z poniższych grup:

– Bezrobotne w rozumieniu ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy;

i/ lub

– Młodocianych, o których mowa w przepisach prawa pracy, w celu przygotowania zawodowego;

i/ lub

– Niepełnosprawne w rozumieniu ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych;

i/ lub

– Inne osoby niż określone w pkt a), b) lub c), o których mowa w ustawie z dnia 13 czerwca 2003 r. o zatrudnieniu socjalnym (t. j. Dz. U. 2019 poz. 217) lub we właściwych przepisach państw członkowskich Unii Europejskiej lub Europejskiego Obszaru Gospodarczego.

Punkty w zakresie niniejszego Kryterium nr 2 zostaną przyznane w następujący sposób:

☐ ZATRUDNIĘ nową osobę/ osoby z grup wskazanych powyżej do realizacji zamówienia - 5 punktów*;

☐ NIE ZATRUDNIĘ nowej osoby/ osób z grup wskazanych powyżej do realizacji zamówienia - 0 punktów*.

* **Należy wskazać/zaznaczyć właściwe (x lub ✓ itp.)- jeżeli dotyczy.**

Ocena w zakresie tego kryterium zostanie dokonana na podstawie wypełnionego **Załącznika nr 2** do SIWZ i złożonej w nim deklaracji Wykonawcy. Maksymalna liczba punktów, która może zostać przyznana Wykonawcy w ocenie ww. kryterium wynosi 5 pkt.

W przypadku nie zaznaczenia żadnej z odpowiedzi Wykonawca otrzyma 0 pkt. Maksymalna liczba punktów, która może zostać przyznana Wykonawcy w ocenie ww. kryterium wynosi 5 pkt. Zakres deklaracji wymagany jest przez cały okres realizacji zamówienia.

Wykonawca oferty najkorzystniejszej, dla potwierdzenia powyższej deklaracji, zobowiązany będzie przed podpisaniem umowy, przedłożyć Zamawiającemu wykaz tych osób, oraz m.in.: imię i nazwisko, liczba osób, z jakiej grupy są to osoby; informacje potwierdzające przesłanki wskazane przez Wykonawcę w Kryterium nr 3 (Klauzula społeczna) winny być możliwe do zidentyfikowania w przypadku ewentualnej kontroli przez organy uprawnione do tego typu czynności. Oświadczenie stanowić będzie załącznik do umowy.

3. Punktacja przyznawana ofertom w poszczególnych kryteriach będzie liczona z dokładnością do dwóch miejsc po przecinku. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.
4. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiadać będzie wszystkim wymaganiom przedstawionym w ustawie PZP, oraz w SIWZ i zostanie oceniona jako najkorzystniejsza w oparciu o podane kryteria wyboru.
5. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert

wybiera ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie lub koszcie, zamawiający wzywa wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych.

6. Zamawiający nie przewiduje unieważnienia postępowania o udzielenie zamówienia na podstawie art. 93 ust. 1a ustawy Pzp.
7. Zamawiający poprawi w tekście oferty omyłki wskazane w art. 87 ust. 2 ustawy, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
8. Jeżeli zaoferowana cena, lub ich istotne części składowe, wydają się rażąco niskie w stosunku do przedmiotu zamówienia i budzą wątpliwości zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez zamawiającego lub wynikającymi z odrębnych przepisów, zamawiający zwraca się o udzielenie wyjaśnień, w tym złożenie dowodów, dotyczących wyliczenia ceny, w szczególności w zakresie przesłanek wskazanych w art. 90 ust. 1 ustawy Pzp.
9. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny, spoczywa na Wykonawcy.
10. Zamawiający odrzuca ofertę Wykonawcy, który nie udzielił wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz ze złożonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.
11. Jako najkorzystniejsza zostanie wybrana oferta, która uzyska najwyższą ocenę zgodnie z kryteriami oceny ofert określonymi w pkt 2 niniejszego rozdziału SIWZ.
12. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiadać będzie wszystkim wymaganiom przedstawionym w ustawie PZP, oraz w SIWZ i zostanie oceniana jako najkorzystniejsza w oparciu o podane kryteria oceny ofert.
13. Zamawiający informuje niezwłocznie wszystkich Wykonawców o:
    1) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres, jeżeli jest miejscem wykonywania działalności wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy, jeżeli są miejscami wykonywania działalności wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,
    2) Wykonawcach, którzy zostali wykluczeni,
    3) Wykonawcach, których oferty zostały odrzucone, powodach odrzucenia oferty, a w przypadkach, o których mowa w art. 89 ust. 4 i 5, braku równoważności lub braku spełniania wymagań dotyczących wydajności lub funkcjonalności,
    4) unieważnieniu postępowania,
    - podając uzasadnienie faktyczne i prawne.
14. Zamawiający udostępnia informacje, o których mowa w pkt 13 ppkt 1 i 4 niniejszego rozdziału SIWZ, na stronie internetowej.
15. W przypadku wystąpienia przesłanek, o których mowa w art. 93 ust. 1 ustawy Zamawiający unieważnia postępowanie.
16. O unieważnieniu postępowania Zamawiający zawiadomi równocześnie wszystkich Wykonawców, którzy:

a. ubiegali się o udzielenie zamówienia, - w przypadku unieważnienia postępowania przed upływem terminu składania ofert,
b. złożyli oferty - w przypadku unieważnienia postępowania po upływie terminu składania ofert

- podając uzasadnienie faktyczne i prawne.

XIV. Informacje o formalnościach, jakie powinny być dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.

1. Z Wykonawcą, którego oferta zostanie uznana za najkorzystniejszą, Zamawiający podpisze umowę w formie pisemnej pod rygorem nieważności, zgodnie z projektem umowy, stanowiącym **Załącznik nr 4 SIWZ,** nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, nie później jednak niż przed upływem terminu związania ofertą, z zastrzeżeniem art. 94 ust. 2 ustawy Pzp.
2. Zawarta umowa będzie jawna i będzie podlegała udostępnianiu na zasadach określonych w przepisach o dostępie do informacji publicznej (art. 139 ust. 3 ustawy Pzp).
3. Zawarcie umowy na realizację przedmiotu zamówienia nastąpi w siedzibie Zamawiającego. Wykonawca, który złożył ofertę najkorzystniejszą, w zaproszeniu do zawarcia umowy zostanie poinformowany o miejscu i terminie zawarcia umowy.
4. Zawarcie umowy może również nastąpić, w taki sposób, iż Zamawiający prześle Wykonawcy (na jego koszt) wypełnioną umowę w odpowiedniej liczbie egzemplarzy, a Wykonawca odeśle podpisane egzemplarze w możliwie najwcześniejszym terminie Zamawiającemu. Następnie Zamawiający po podpisaniu umowy odeśle Wykonawcy należny mu egzemplarz umowy. W tym przypadku datą zawarcia umowy będzie dzień podpisania umowy przez Zamawiającego.
5. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
6. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający może żądać przed zawarciem umowy przedstawienia umowy regulującej współpracę tych Wykonawców. Umowa taka winna określać strony umowy, cel działania, sposób współdziałania, zakres prac przewidzianych do wykonania każdemu z nich, solidarną odpowiedzialność za wykonanie zamówienia, oznaczenie czasu trwania konsorcjum (obejmującego okres realizacji przedmiotu zamówienia, gwarancji i rękojmi), wykluczenie możliwości wypowiedzenia umowy konsorcjum przez któregokolwiek z jego członków do czasu wykonania zamówienia.
7. Postanowienia ustalone w projekcie umowy nie podlegają negocjacjom.
8. Formalności, które muszą być dopełnione po wyborze oferty w celu podpisania umowy:
   Wykonawca pod rygorem stwierdzenia uchylania się od zawarcia umowy, najpóźniej w dniu podpisania umowy:
   1) Ma obowiązek przedstawić Zamawiającemu umowę konsorcjum (list intencyjny).

2) Wskaże Zamawiającemu wszystkie składniki oferty cenowej w wartości netto oferty cenowej oraz dane osobowe, które zostaną przeniesione do umowy.
3) Wskaże parametry techniczne wymagane zgodnie z opisem przedmiotu zamówienia oraz wskaże producenta nazwę/ rodzinę zaoferowanego oprogramowania.
4) Wykonawca musi dysponować co najmniej jedną osobą posiadającą uprawnienia (certyfikaty Eset Client Security Administrator, Eset Network Client Security Administrator, Eset Network Security Managment Administraror) w zakresie instalacji i konfiguracji oprogramowania, wystawione przez Producenta lub oficjalnego przedstawiciela Producenta. W przypadku rozwiązania równoważnego Wykonawca przedstawi tożsame certyfikaty danego Producenta lub oficjalnego przedstawiciela Producenta. Wykonawca dostarczy w/w dokument w formie skanu oraz wskaże z imienia i nazwiska min. jedną osobę, która dokona instalacji/ aktualizacji oprogramowania dla poszczególnych lokalizacji. Ponadto, w przypadku zaoferowania rozwiązania równoważnego oprogramowania antywirusowego, Wykonawca wskaże z imienia i nazwiska min. jedną osobę, która przeprowadzi obowiązkowe szkolenie pracowników Zamawiającego (4 osoby); posiadającą uprawnienia do tego typu szkoleń, w zakresie administracji oprogramowaniem wraz z udokumentowaniem takich uprawień.
5) Wykonawca zobowiązany jest dostarczyć w/w informacje możliwe jak najbardziej szczegółowo w języku polskim lub z tłumaczeniem na język polski (informacje zwarte w innym języku- tylko za zgodą Zamawiającego), w terminie nie dłuższym niż 7 dni od dnia przesłania do Wykonawcy pisma z zaproszeniem do zawarcia umowy. Niewywiązanie się z w/w termin, zostanie potraktowane jako uchylanie się od zawarcia umowy.

6) W przypadku nieprzekazania, bądź stwierdzenia przez Zamawiającego, że przedstawione dokumenty, oświadczenia, lub informacje, są niezgodne z SIWZ, lub są niewystarczające, aby swoim zakresem potwierdzić wymagania SWIZ, Wykonawca niezwłocznie przekaże stosowne dokumenty, oświadczenia, lub informacje potwierdzające w/w okoliczności i zgodności oferowanych materiałów/ sprzętu z SIWZ i ofertą cenową Wykonawcy, w terminie nie dłuższym niż 3 dni od dnia przesłania do Wykonawca informacji o powyższym. Niewywiązanie się z w/w termin, zostanie potraktowane jako uchylanie się od zawarcia umowy.

7) Wykonawca oferty najkorzystniejszej celem potwierdzenia deklaracji dot. Klauzuli społecznej- Kryterium nr 3, zobowiązany będzie- jeżeli dotyczy, przed podpisaniem umowy, przedłożyć Zamawiającemu wykaz osób, m.in.: imię i nazwisko, liczba osób, z jakiej grupy są to osoby; informacje potwierdzające przesłanki wskazane przez Wykonawcę w Kryterium nr 3 (klauzule społeczne) winny być możliwe do zidentyfikowania w przypadku ewentualnej kontroli przez organy uprawnione do tego typu czynności. Oświadczenie stanowić będzie załącznik do umowy.

XV. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

1. Wykonawca, którego oferta zostanie wybrana, zobowiązany będzie do wniesienia zabezpieczenia należytego wykonania umowy najpóźniej w dniu jej zawarcia, w wysokości **10 % ceny całkowitej brutto podanej w ofercie.**
2. Zabezpieczenie może być wnoszone według wyboru Wykonawcy w jednej lub w kilku następujących formach:
   a) pieniądzu;
   b) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
   c) gwarancjach bankowych;
   d) gwarancjach ubezpieczeniowych;
   e) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t. j. Dz. U. z 2019 r., poz. 310 z późn. zm.).
3. Zamawiający **nie wyraża** zgody na wniesienie zabezpieczenia w formach określonych art. 148 ust. 2 ustawy PZP.
4. W przypadku wniesienia zabezpieczenia w formie pieniężnej Zamawiający przechowa je na oprocentowanym rachunku bankowym.
5. Z treści zabezpieczenia przedstawionego w formie gwarancji/ poręczenia winno wynikać, że bank, ubezpieczyciel, poręczyciel zapłaci, na rzecz Zamawiającego w terminie maksymalnie 30 dni od pisemnego żądania kwotę zabezpieczenia, na pierwsze wezwanie Zamawiającego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie Zamawiającego jest uzasadnione czy nie.
6. W przypadku, gdy zabezpieczenie, będzie wnoszone w formie innej niż pieniądz, Zamawiający zastrzega sobie prawo do akceptacji projektu ww. dokumentu.
7. Zamawiający zwróci zabezpieczenie w terminie do 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane.

XVI. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli Zamawiający wymaga od Wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach.

1. **Projekt umowy stanowi** Załącznik nr 4 **do SIWZ.**
2. Zakazuje się zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, chyba że zmiany zostały przewidziane w ogłoszeniu o zamówieniu lub specyfikacji istotnych warunków zamówienia w postaci jednoznacznych postanowień umownych, które określają ich zakres, w szczególności możliwość zmiany wysokości wynagrodzenia wykonawcy, i charakter oraz warunki wprowadzenia zmian**.**
3. **Zamawiający przewiduje możliwość wprowadzenia zmian, które zostały określone w Projekcie umowy, stanowiącym załącznik nr 4 do SIWZ.**
4. Nie stanowi zmiany umowy w rozumieniu art. 144 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t. j. Dz. U. z 2019 r. poz. 1843):

- Zmiana danych związanych z obsługą administracyjno-organizacyjną umowy (np. zmiana nr rachunku bankowego),
- Zmiana danych teleadresowych oraz nazw Stron.

XVII. Pouczenie o środkach ochrony prawnej.

1. Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes prawny w uzyskaniu przedmiotowego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Prawo zamówień publicznych na podstawie art. 180 ust. 2 ustawy Pzp przysługuje odwołanie wyłącznie wobec czynności:
    1) wyboru trybu negocjacji bez ogłoszenia, zamówienia z wolnej ręki lub zapytania o cenę;
    2) określenia warunków udziału w postępowaniu;
    3) wykluczenia odwołującego z postępowania o udzielenie zamówienia;
    4) odrzucenia oferty odwołującego;
    5) opisu przedmiotu zamówienia;
    6) wyboru najkorzystniejszej oferty.
2. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy Prawo zamówień publicznych, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
3. Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
4. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
5. Odwołanie wnosi się w terminach wskazanych w art. 182 ustawy Prawo zamówień publicznych.
6. Wykonawca może w terminie przewidzianym do wniesienia odwołania poinformować Zamawiającego o niezgodnej z przepisami ustawy czynności podjętej przez niego lub zaniechaniu czynności, do której jest on zobowiązany na podstawie ustawy, na które nie przysługuje odwołanie z art. 180 ust. 2 ustawy Pzp.

XVIII. Załączniki

ZAŁĄCZNIK NR 1	Szczegółowy opis przedmiotu zamówienia
ZAŁĄCZNIK NR 2	Formularz ofertowy
ZAŁĄCZNIK NR 3	Oświadczenie o braku podstaw do wykluczenia
ZAŁĄCZNIK NR 4	Projekt umowy

ZAŁĄCZNIK NR 5 Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp.

Niniejsza SIWZ została przedłożona przez Komisję Przetargową do zatwierdzenia Kierownikowi Zamawiającego:

Skład i funkcja osób w Komisji Przetargowej:

	Imię i nazwisko:
Przewodniczący Komisji	Piotr Rzetecki
Sekretarz Komisji	Pan Marcin Białowąs
Członek Komisji	Pan Michał Potrzebny
Członek Komisji	Pan Marcin Nowakowski
Członek Komisji	Pan Dariusz Hołda

Zatwierdzam:

Dyrektor Wojewódzkiego Urzędu Pracy w Szczecinie

Andrzej Przewoda

ZAŁĄCZNIK NR 1	Szczegółowy opis przedmiotu zamówienia

Przedłużenie aktualizacji Eset Endpoint Antivirus Suite lub równoważnego programu antywirusowego, na okres od 22-12-2019r. do 21-12-2020r. Konto użytkownika: EAV-37307887. Aktualizacje baz sygnatur wirusów i oprogramowania.

Ilość posiadanych licencji z FP: 170.

Ilość posiadanych licencji z EFS'u: 100.

Ilość posiadanych licencji z FGŚP: 14.

Łącznie: 314.

Usługa aktualizacji oprogramowania ESET do najnowszej wersji na serwerze klienta oraz wszystkich jednostkach komputerowych w ilości około 314 szt. Usługa aktualizacji musi odbyć się w siedzibie klienta na ul. Mickiewicza 41, ul. Żubrów 3 oraz zdalnie w Filii WUP w Koszalinie.

Aktualizację przeprowadzić będzie można w dniach od Poniedziałku do Piątku w godzinach 7:30 – 15:30 z wyłączeniem dni ustawowo wolnych od pracy.

W przypadku równoważnego oprogramowania antywirusowego, obowiązkowe jest przeszkolenie pracowników Zamawiającego (4 osoby) przez osobę posiadającą uprawnienia do tego typu szkoleń, w zakresie administracji oprogramowaniem. Termin realizacji nie ulega zmianie- zgodnie z deklaracją w ofercie cenowej- liczona jako całość przedmiotu zamówienia- max 14 dni kalendarzowych od dnia zawarcia umowy lub deklaracją złożoną w ofercie cenowej.

W przypadku oprogramowania równoważnego, Wykonawca max do 14 dni kalendarzowych od dnia zawarcia umowy lub deklaracją złożoną w ofercie cenowej winien :

1. Zaprojektować nową architekturę rozwiązania i jej implementację obok już istniejącej starej architektury (przed końcem działania starej licencji trzeba przygotować do uruchomienia nowe środowisko).

2. Przeprowadzić odinstalowanie starego klienta antywirusowego na 314 stacjach oraz agentów działających na stacjach.

3. Przeprowadzić konwersję polis antywirusowych obowiązujących na starym serwerze antywirusowym do nowego serwera antywirusowego.

4. Przeprowadzić konwersję konfiguracji stacji antywirusowej w 3 profilach: skanowania z menu kontekstowego, skanowania z inteligentnym wyborem obiektów, skanowania dokładnego wszystkich plików. Konfiguracja musi zostać przekonwertowana dla 3 modułów: skanowania komputera, skanowania poczty e-mail, ochrony dokumentów.

5. Przeprowadzić konwersję konfiguracji serwerowych stacji Windows i Linux również w 3 profilach i 3 modułach.

Specyfikacja programu równoważnego:

Ochrona stacji roboczych - Windows

1. Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows 8/Windows 8.1/Windows 10/

2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.

3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.

4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.

5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.

Ochrona antywirusowa i antyspyware

6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

8. Wbudowana technologia do ochrony przed rootkitami.

9. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

11. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.

12. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.

13. 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).

14. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

15. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.

16. Możliwość skanowania dysków sieciowych i dysków przenośnych.

17. Skanowanie plików spakowanych i skompresowanych.

18. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

19. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.

20. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.

21. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

22. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.

23. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.

24. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.

25. 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.

26. Wbudowany konektor dla programów MS Outlook.

27. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook.

28. 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).

29. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

30. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

31. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.

32. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.

33. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej

przez administratora.

34. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

35. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

36. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.

37. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.

38. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.

39. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.

40. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.

41. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.

42. 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.

43. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie- z użyciem jednej lub obu metod jednocześnie.

44. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.

45. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.

46. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

47. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

48. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy

próbie dostępu do konfiguracji, był proszony o jego podanie.

49. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.

50. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.

51. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.

52. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.

53. 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 zagrożeń.

54. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.

55.System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.

56. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

57. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.

58. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

59. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.

60. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.

61. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi

odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

62. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.

63. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

64. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

65. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

66. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.

67. Oprogramowanie musi posiadać zaawansowany skaner pamięci.

68. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.

69. 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 procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

70. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.

71. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.

72. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

73. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.

74. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.

75. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.

76. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.

77. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).

78. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

79. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.

80. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.

81. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.

82. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.

83. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

84. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.

85. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

86. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.

87. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.

88. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.

89. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym

automatycznie zostaną przywrócone dotychczasowe ustawienia.

90. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.

91. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.

92. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.

93. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.

94. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.

95. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.

96. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

97. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.

98. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.

99. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.

100. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.

101. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

102. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.

103.Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

104. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

105. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.

106. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

Ochrona stacji roboczych - Mac OSX

1. Procesor 32-bit (x86) / 64-bit (x64), Intel®.

2. Pełne wsparcie dla systemów Mac OS X 10.9 lub nowszy.

3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.

4. Pomoc w programie (help) w języku polskim oraz angielskim.

5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

6. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.

7. 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.

8. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

10. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).

11. Możliwość skanowania dysków sieciowych i dysków przenośnych.

12. Skanowanie plików spakowanych i skompresowanych.

13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

14. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

15. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.

16. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.

17. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.

18. Możliwość wykonania skanowania i wysłania pliku do analizy z poziomu menu kontekstowego.

19. Aktualizacje modułów analizy heurystycznej.

20. 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 mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

21. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

22. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

23. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

24. Ochrona przed atakami typu „phishing”.

25. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, karty sieciowe, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne.

26. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

27. Aktualizacja modułów programu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy serwera HTTP.

28. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

29. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).

30. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.

31. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

32. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.

33. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.

34. Program musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.

35. Program musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.

36. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy” na modyfikację konfiguracji programu.

37. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

38. Możliwość zdalnego zarządzania programem z poziomu Administracji zdalnej.

39. Ochrona poczty mail:

• skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej niezależnie od programu pocztowego.

• skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

• automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

• możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.

• możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.

• możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

Aktualizacje sygnatur:

1. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.

2. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.

3. Aplikacja ma posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją. Konfiguracja i zdalne zarządzanie.

4. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie.

5. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.

6. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.

7. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.

8. Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów:

a. za pomocą kodu QR,

b. za pomocą unikatowego łącza,

c. za pomocą wiadomości e-mail,

W ramach aktywacji za pomocą kodu QR musi istnieć możliwość aktywacji w trybie właściciela urządzenia (Android Enterprise Device Owner).

Ochrona serwera Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2008 SP2 (oparty na procesorze x86 i x64), Server Core (Microsoft Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016).

2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.

3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

5. Wbudowana technologia do ochrony przed rootkitami i exploitami.

6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

8. 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).

9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

10. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.

11. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.

12. Możliwość skanowania dysków sieciowych i dysków przenośnych.

13. Skanowanie plików spakowanych i skompresowanych.

14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

15. Aplikacja powinna wspierać mechanizm klastrowania.

16. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

17. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

b. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

d. tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

e. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

18. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

19. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.

20. Oprogramowanie musi posiadać zaawansowany skaner pamięci.

21. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.

22. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.

23. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.

24. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

25. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub

model urządzenia.

26. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

27. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.

28. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.

29. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

30. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

31. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

32. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.

33. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.

34. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.

35. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.

36. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.

37. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).

38. 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.

39. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.

40. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do

laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez 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. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.

45. 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.

46. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.

47. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.

48. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.

49. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.

50. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.

51. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.

52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.

53. 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 procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

54. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.

55. 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.

56. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

57. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.

58. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.

59. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.

60. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.

61. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).

62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

63. Aplikacja musi wspierać skanowanie magazynu Hyper-V.

64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.

65. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.

66. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

67. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.

68. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.

70. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem

aktywności wirusów sieciowych.

71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

72. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.

73. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

74. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.

75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.

77. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

Administracja zdalna

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2008 R2, 2012, 2016, 2019 oraz systemach Linux.

2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.

3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.

4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.

5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.

6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.

7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.

9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.

10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.

11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.

12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

13. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.

14. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.

15. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na

podstawie unikatowego identyfikatora sprzętowego stacji.

17. Serwer administracyjny musi posiadać możliwość podłączenia 500 hostów.

18. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.

19. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

20. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.

21. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.

22. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.

23. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.

24. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.

25. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.

26. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.

27. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.

28. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer

proxy, moduł zarządzania urządzeniami mobilnymi, host agenta wirtualnego.

29. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.

30. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.

31. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.

32. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.

33. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.

34.Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.

35. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.

36. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.

37. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.

38. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.

39. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.

40. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.

41. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.

42. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

43. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów,

raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.

45.Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.

46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.

47. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.

48. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.

49. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.

50. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.

51. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.

52. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

53. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

54. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

55. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.

56. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.

57. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.

58. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.

59. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.

60. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.

61. Serwer administracyjny musi posiadać minimum 170 szablonów raportów, przygotowanych przez producenta.

62.Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.

63. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.

64. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.

65. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.

66. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.

67. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.

68. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV oraz PS.

69. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.

70. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.

71. Powiadomienia mailowe mają być wysyłane w formacie HTML.

72. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.

73. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.

74. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.

75. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.

76. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.

77. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.

78. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.

79. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.

80. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.

81. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

82. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.

83. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.

84. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.

85. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.

86. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.

87. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.

Warunek zawarcia umowy. Wykonawca musi dysponować co najmniej jedną osobą posiadającą uprawnienia (certyfikaty Eset Client Security Administrator, Eset Network Client Security Administrator,

Eset Network Security Managment Administraror) w zakresie instalacji i konfiguracji wystawione przez Producenta lub oficjalnego przedstawiciela Producenta. W przypadku rozwiązania równoważnego Wykonawca przedstawi tożsame certyfikaty danego Producenta lub oficjalnego przedstawiciela Producenta.

ZAŁĄCZNIK NR 2	FORMULARZ OFERTOWY

A. DANE WYKONAWCY:

Ja (My), niżej podpisany (ni)

.....

działając w imieniu i na rzecz:

…….....

……

(pełna nazwa Wykonawcy)

.....

(adres siedziby Wykonawcy)

REGON..... Nr NIP

.....

Nr konta bankowego: .....

nr telefonu ..... nr faxu .....

e-mail do kontaktu: .....

B. ŁĄCZNA CENA UMOWNA:

w odpowiedzi na ogłoszenie o wszczęciu postępowania prowadzonego w trybie przetargu nieograniczonego o wartości zamówienia mniejszej od kwot określonych w przepisach wydanych na podstawie art. 11 ust. 8 pn.: „Dostawa aktualizacji oprogramowania antywirusowego na potrzeby WUP", oferuję wykonanie zamówienia zgodnie z opisem przedmiotu zamówienia i na warunkach płatności określonych w SIWZ za łączną cenę umowną

brutto*: ……zł,

* **ŁĄCZNA CENA UMOWNA BRUTTO** stanowi całkowite wynagrodzenie Wykonawcy, uwzględniające wszystkie koszty związane z realizacją przedmiotu zamówienia zgodnie z niniejszą SIWZ.

C. OŚWIADCZENIA:

1) Oświadczam(y), że przedmiot zamówienia zrealizujemy **w zakresie i w terminie do …….. dni kalendarzowych od dnia zawarcia umowy (maksymalny termin realizacji przedmiotu zamówienia wynosi 14 dni kalendarzowych od dnia zawarcia umowy, zgodnie z Kryterium nr 2).** W przypadku nie wpisania żadnej wartości, wpisania mniej niż 1 dni, lub ułamków lub innej wartości niż pełne liczby od 1 do 14, Zamawiający uzna, że Wykonawca wykona przedmiot umowy w terminie maksymalnym tj. 14 dni kalendarzowych od dnia zawarcia umowy, a punktacja zostanie przyznana w oparciu o wartość 14 dni kalendarzowych

2) **Oświadczamy, iż niniejsza oferta jest zgodna z warunkami i treścią SIWZ, ponadto oferujemy:**

- **w ramach Kryterium nr 3,** zatrudnienie przy realizacji zamówienia nowych osób znajdujących się w trudnej sytuacji na rynku pracy (klauzula społeczna), oświadczam/y, że do realizacji zamówienia (Wykonawca lub Podwykonawca) zatrudni/ zatrudnimy nową osobę/ osoby:
  - Bezrobotne w rozumieniu ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy;
    i/ lub
  - Młodocianych, o których mowa w przepisach prawa pracy, w celu przygotowania zawodowego;
    i/ lub
  - Niepełnosprawne w rozumieniu ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych;
    i/ lub
  - Inne osoby niż określone w pkt a), b) lub c), o których mowa w ustawie z dnia 13 czerwca 2003 r. o zatrudnieniu socjalnym (t. j. Dz.U. 2019 poz. 217) lub we właściwych przepisach państw członkowskich Unii Europejskiej lub Europejskiego Obszaru Gospodarczego,
    w następującym zakresie:

    ☐ ZATRUDNIĘ nową osobę/ osoby z grup wskazanych powyżej do realizacji zamówienia - 5 punktów*;

    ☐ NIE ZATRUDNIĘ nowej osoby/ osób z grup wskazanych powyżej do realizacji zamówienia - 0 punktów*.

    * **Należy wskazać/zaznaczyć właściwe (x lub ✓ itp.)- jeżeli dotyczy.**

3) Oświadczam(y), że jesteśmy związani niniejszą ofertą przez okres 30 dni od upływu terminu składania ofert.
4) Oświadczamy, że zapoznaliśmy się z treścią Specyfikacji Istotnych Warunków Zamówienia i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w niej zawarte.
5) Oświadczamy, że zawarty w Specyfikacji Istotnych Warunków Zamówienia projekt umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku wyboru naszej oferty do jej zawarcia na wyżej wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.
6) Oświadczamy, iż niniejsza oferta jest zgodna z warunkami i treścią SIWZ.
7) Oświadczamy, że uzyskaliśmy wszelkie informacje niezbędne do prawidłowego przygotowania i złożenia niniejszej oferty.

8) Oświadczamy, że w przypadku przyznania nam zamówienia, nie odstąpimy od jego realizacji w przypadku spełnienia przez zamawiającego warunków umowy.

9) Oświadczamy, że oferta nie zawiera/ zawiera (właściwe podkreślić) informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Informacje takie zawarte są w następujących dokumentach:

.....

10) Oświadczam, że jesteśmy:

- ☐ mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem *
- ☐ dużym przedsiębiorstwem *

* w rozumieniu Ustawy z dnia 6 marca 2018 r. Prawo Przedsiębiorców

Uwaga – w przypadku składania oferty wspólnej powyższe oświadczenie należy złożyć dla każdego z wykonawców oddzielnie.

* **Należy wskazać/zaznaczyć właściwe (x lub ✓ itp.)**

11) Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

D. PODWYKONAWCY:

Podwykonawcom zamierzam powierzyć poniższe części zamówienia (Jeżeli jest to wiadome, należy podać również dane proponowanych podwykonawców)

1) .....

2) .....

E. SPIS TREŚCI:

Integralną część oferty stanowią następujące dokumenty:

1) .....

2) .....

Jednocześnie wykonawca wskazuje zgodnie z § 10 Rozporządzenia Ministra Rozwoju z 26 lipca 2016 roku w sprawie rodzajów dokumentów jakich może żądać zamawiający (…) następujące oświadczenia lub dokumenty, które znajdują się w posiadaniu zamawiającego / są dostępne pod poniższymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych:

1) .....

2) .....

Oferta została złożona na ..... kolejno ponumerowanych stronach.

……	.....
pieczęć Wykonawcy	podpis upoważnionego przedstawiciela Wykonawcy

ZAŁĄCZNIK NR 3	OŚWIADCZENIE O BRAKU PODSTAW DO WYKLUCZENIA

WUP.XVA.322.265.MBi.2019

.....
(pieczęć Wykonawcy)

Oświadczenie Wykonawcy

składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.
Prawo zamówień publicznych

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

„Dostawa aktualizacji oprogramowania antywirusowego na potrzeby WUP"

1. OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust 1 pkt 12-22 ustawy Pzp.
2. Oświadczam, że brak jest podstaw do wykluczenia mnie z postępowania na podstawie art. 24 ust. 5 pkt 1 ustawy Pzp.

..... , dn. ....

(miejscowość, data) Podpis Wykonawcy
(podpisy osób uprawnionych
do reprezentowania Wykonawcy)

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 lub art. 24 ust. 5 pkt. 1 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze[1]:
……

. ..... , dn. ....

(miejscowość, data) Podpis Wykonawcy
(podpisy osób uprawnionych
do reprezentowania Wykonawcy)

[1] UWAGA: Niniejsze oświadczenie składa Wykonawca, tylko w sytuacji wystąpienia niniejszych przesłanek. W sytuacji braku ich wystąpienia nie należy wypełniać wskazanego miejsca.

2. OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY NIEBĘDĄCEGO PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że następujący/e podmiot/y, będący/e podwykonawcą/ami: …… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*, nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia[2].

..... , dn. ....

(miejscowość, data) Podpis Wykonawcy
(podpisy osób uprawnionych
do reprezentowania Wykonawcy)

3. OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

..... , dn. ....

(miejscowość, data) Podpis Wykonawcy
(podpisy osób uprawnionych

[2] UWAGA: Niniejsze oświadczenie składa Wykonawca, tylko w sytuacji wystąpienia niniejszych przesłanek. W sytuacji braku ich wystąpienia nie należy wypełniać wskazanego miejsca.

ZAŁĄCZNIK NR 5	**OŚWIADCZENIE O PRZYNALEŻNOŚCI LUB BRAKU PRZYNALEŻNOŚCI DO TEJ SAMEJ GRUPY KAPITAŁOWEJ, O KTÓREJ MOWA W ART. 24 UST. 1 PKT 23 USTAWY PZP.**

WUP.XVA.322.265.MBi.2019

.....
(pieczęć Wykonawcy)

Oświadczenie[3] zgodnie z art. 24 ust. 11 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2019 r. poz. 1843):

1. **Oświadczam, że należę/należymy** do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP **–** tj. do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz. U. z 2018 r. poz. 798) **– z następującym/cymi Wykonawcą/Wykonawcami,** którzy złożyli Oferty w ramach niniejszego postępowania:

Nr oferty	Wykonawca	Adres Wykonawcy

..... , dnia ..... …….....
(podpis osoby upoważnionej do reprezentacji)

..... , dnia ..... …….....
(podpis osoby upoważnionej do reprezentacji)

[3] Należy wypełnić punkt 1 lub 2.

2. **Oświadczam, że[4]:**

☐ **nie należę/należymy** do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP **–** tj. do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz. U. z 2018 r. poz. 798) **– z żadnym z Wykonawców**, którzy złożyli Oferty w ramach niniejszego postępowania

LUB

☐ **nie należę/należymy do żadnej grupy kapitałowej**, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz. U. z 2018 r. poz. 798).

..... , dnia ..... …….....
(podpis osoby upoważnionej do reprezentacji)

..... , dnia ..... …….....
(podpis osoby upoważnionej do reprezentacji)

[4] W przypadku wypełnienia pkt 2 należy zaznaczyć właściwe pole