Nr sprawy 8/09

Specyfikacja Istotnych Warunków Zamówienia

ZAMAWIAJĄCY:

Gmina Miasto Szczecin – Biuro ds. Zamówień Publicznych
Urzędu Miasta Szczecin
Pl. Armii Krajowej 1
70-456 Szczecin
(pok. nr 397)

ZAPRASZA DO ZŁOŻENIA OFERTY W POSTĘPOWANIU PROWADZONYM W TRYBIE

PRZETARGU NIEOGRANICZONEGO NA DOSTAWY

O WARTOŚCI ZAMÓWIENIA MNIEJSZEJ OD KWOT OKREŚLONYCH W PRZEPISACH WYDANYCH NA PODSTAWIE ART. 11 UST. 8 NA:

„Dostawę oprogramowania antywirusowego dla Urzędu Miasta Szczecin”

SPIS TREŚCI :

Załączniki:

Podstawa prawna: Ustawa z dnia 29.01.2004r. Prawo zamówień publicznych (t.j. Dz. U. z 2007r. nr 223, poz. 1655 z późn. zm.), zwana dalej ustawą.

Nr sprawy 8/09

ROZDZIAŁ I Forma oferty

1. Na **ofertę** składają się: oferta cenowa oraz wszystkie pozostałe wymagane dokumenty (w tym oświadczenia, załączniki itp.) zgodnie z rozdziałem V specyfikacji istotnych warunków zamówienia (siwz).
2. Wykonawcy sporządzą oferty zgodnie z wymaganiami siwz.
3. Oferta cenowa musi być sporządzona na formularzu oferty, według wzoru stanowiącego **załącznik nr 1** do siwz.
4. Oferta musi być sporządzona w języku polskim, na maszynie do pisania, komputerze lub ręcznie długopisem. Oferty nieczytelne zostaną odrzucone.
5. Oferta musi być podpisana przez osoby upoważnione do składania oświadczeń woli w imieniu wykonawcy. Upoważnienie do podpisania oferty musi być dołączone do oferty **w oryginale lub kopii poświadczonej za zgodność z oryginałem przez notariusza,** o ile nie wynika ono z innych dokumentów załączonych przez wykonawcę.
6. W przypadku, gdy wykonawca składa kopię jakiegoś dokumentu, musi być ona poświadczona za zgodność z oryginałem przez wykonawcę (wykonawca składa własnoręczny podpis poprzedzony dopiskiem „za zgodność"), **z zastrzeżeniem pkt 5 oraz Rozdział III pkt 2 niniejszej siwz**. Jeżeli do reprezentowania wykonawcy upoważnione są łącznie dwie lub więcej osób, kopie dokumentów muszą być potwierdzone za zgodność z oryginałem przez te osoby.
7. Jeżeli któryś z wymaganych dokumentów składanych przez wykonawcę jest sporządzony w języku obcym dokument taki należy złożyć wraz z tłumaczeniem na język polski poświadczonym przez wykonawcę. Dokumenty sporządzone w języku obcym bez wymaganych tłumaczeń nie będą brane pod uwagę.
8. Zaleca się, aby wszystkie strony oferty były ponumerowane. Ponadto, wszelkie miejsca, w których wykonawca naniósł zmiany, muszą być przez niego parafowane.
9. Wykonawca składa tylko jedną ofertę.
10. Zamawiający nie dopuszcza składania ofert wariantowych.
11. Zamawiający **dopuszcza składanie ofert częściowych**. Wykonawca może złożyć ofertę na jedną, dwie lub trzy grupy zamówienia.
12. Zamawiający nie przewiduje udzielania zamówień uzupełniających.
13. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
14. Zaleca się, aby wykonawca zamieścił ofertę w zewnętrznej i wewnętrznej kopercie z tym, że:
    1) zewnętrzna koperta powinna być oznaczona w następujący sposób: **Gmina Miasto Szczecin – Biuro ds. Zamówień Publicznych, Pl. Armii Krajowej 1, 70-456 Szczecin, pok. nr 397, przetarg nieograniczony, "oferta na Dostawę oprogramowania antywirusowego dla Urzędu Miasta Szczecin"** oraz **„nie otwierać przed 16.02.2009 r. godz. 11 00"** - bez nazwy i pieczątki wykonawcy;
    2) koperta wewnętrzna powinna zawierać ofertę i być zaadresowana na wykonawcę, tak aby można było odesłać ofertę w przypadku jej wpłynięcia po terminie.
15. Jeżeli oferta wykonawcy nie będzie oznaczona w sposób wskazany w pkt 14, zamawiający nie będzie ponosić żadnej odpowiedzialności za nieterminowe wpłynięcie oferty. Zamawiający nie będzie ponosić odpowiedzialności za nieterminowe złożenie oferty w szczególności w sytuacji, gdy oferta nie zostanie złożona do pokoju wskazanego w pkt 14 ppkt 1) lecz wpłynie do kancelarii Urzędu Miasta.

ROZDZIAŁ II Zmiana, wycofanie i zwrot oferty

1. Wykonawca może wprowadzić zmiany oraz wycofać złożoną przez siebie ofertę przed terminem składania ofert.
   1) w przypadku wycofania oferty, wykonawca składa pisemne oświadczenie, że ofertę swą wycofuje, w zamkniętej kopercie zaadresowanej jak w rozdziale I pkt 14 ppkt 1) z dopiskiem „wycofanie".
   2) w przypadku zmiany oferty, wykonawca składa pisemne oświadczenie, iż ofertę swą zmienia, określając zakres i rodzaj tych zmian a jeśli oświadczenie o zmianie pociąga za sobą konieczność wymiany czy też przedłożenia nowych dokumentów – wykonawca winien dokumenty te złożyć .
      Powyższe oświadczenie i ew. dokumenty należy zamieścić w kopercie wewnętrznej i zewnętrznej, oznaczonych jak w rozdziale I pkt 14 ppkt 1) i 2) przy czym koperta zewnętrzna powinna mieć dopisek „zmiany".
2. Wykonawca nie może wprowadzić zmian do oferty oraz wycofać jej po upływie terminu składania ofert.
3. Oferty złożone po terminie składania zamawiający zwraca wykonawcom bez otwierania, po upływie terminu do wniesienia protestu.

ROZDZIAŁ III Oferty wspólne

1. Wykonawcy składający ofertę wspólną ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i zawarcia umowy.
2. Pełnomocnictwo, o którym mowa w pkt 1 musi znajdować się w ofercie wspólnej wykonawców. **Pełnomocnictwo musi być złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem przez notariusza**.
3. Pełnomocnik pozostaje w kontakcie z zamawiającym w toku postępowania; zwraca się do zamawiającego z wszelkimi sprawami i do niego zamawiający kieruje informacje, korespondencję, itp..
4. Oferta wspólna, składana przez dwóch lub więcej wykonawców, powinna spełniać następujące wymagania:
   1) oferta wspólna powinna być sporządzona zgodnie z siwz;
   2) sposób składania dokumentów w ofercie wspólnej:
      a) dokumenty, dotyczące własnej firmy, takie jak np.: odpis z właściwego rejestru albo zaświadczenie o wpisie do ewidencji działalności gospodarczej, – składa każdy z wykonawców składających ofertę wspólną w imieniu swojej firmy;
      b) dokumenty wspólne takie jak np.: oferta cenowa, oświadczenia, harmonogramy itp. składa pełnomocnik wykonawców w imieniu wszystkich wykonawców składających ofertę wspólną,
      c) wadium w formie innej niż pieniężna musi być wystawione na wszystkich wykonawców składających ofertę wspólną.
5. Wspólnicy spółki cywilnej są traktowani jak wykonawcy składający ofertę wspólną i mają do nich zastosowanie zasady określone w pkt 1 – 4 niniejszego rozdziału.
6. Przed podpisaniem umowy (w przypadku wygrania postępowania) wykonawcy składający ofertę wspólną będą mieli obowiązek przedstawić zamawiającemu umowę konsorcjum, zawierającą, co najmniej:

1) zobowiązanie do realizacji wspólnego przedsięwzięcia gospodarczego obejmującego swoim zakresem realizację przedmiotu zamówienia,
2) określenie zakresu działania poszczególnych stron umowy,
3) czas obowiązywania umowy, który nie może być krótszy, niż okres obejmujący realizację zamówienia oraz czas trwania gwarancji jakości i rękojmi.

ROZDZIAŁ IV Jawność postępowania

1. Zamawiający prowadzi protokół postępowania.
2. Protokół postępowania wraz z załącznikami jest jawny. Protokół i załączniki do protokołu udostępnia się na wniosek, po dokonaniu wyboru najkorzystniejszej oferty lub unieważnieniu postępowania, z tym że oferty udostępnia się od chwili ich otwarcia.
3. Udostępnienie protokołu lub załączników może nastąpić przez wgląd w miejscu wyznaczonym przez zamawiającego, przesłanie kopii pocztą, faksem lub drogą elektroniczną, zgodnie z wyborem wnioskodawcy wskazanym we wniosku.
4. Bez zgody zamawiającego wnioskodawca w trakcie wglądu do protokołu lub załączników w miejscu wyznaczonym przez zamawiającego nie może samodzielnie kopiować lub utrwalać za pomocą urządzeń lub środków technicznych służących do utrwalania obrazu treści złożonych ofert.
5. Jeżeli przesłanie kopii protokołu lub załączników zgodnie z wyborem wnioskodawcy jest z przyczyn technicznych utrudnione, w szczególności z uwagi na ilość żądanych do przesłania dokumentów, zamawiający informuje o tym wnioskodawcę i wskazuje sposób, w jaki mogą być one udostępnione.
6. Jeżeli udostępnianie protokołu lub załączników będzie się wiązało z koniecznością poniesienia dodatkowych kosztów, związanych z wskazanym przez wnioskodawcę sposobem udostępniania lub koniecznością przekształcenia protokołu lub załączników koszty te pokrywa wnioskodawca.
7. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą one być udostępniane.
8. W przypadku zastrzeżenia informacji wykonawca ma obowiązek wydzielić z oferty informacje stanowiące tajemnicę jego przedsiębiorstwa i oznaczyć je klauzulą „nie udostępniać. Informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. nr 153, poz. 1503 z późniejszymi zmianami)”.
9. W sytuacji, gdy wykonawca zastrzeże w ofercie informacje, które nie stanowią tajemnicy przedsiębiorstwa lub są jawne na podstawie przepisów ustawy Prawo zamówień publicznych lub odrębnych przepisów, informacje te będą podlegały udostępnieniu na takich samych zasadach, jak pozostałe niezastrzeżone dokumenty.

ROZDZIAŁ V Wymagane dokumenty potwierdzające spełnianie warunków udziału w postępowaniu, opis warunków oraz sposób oceny ich spełniania. Inne dokumenty wymagane w ofercie.

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

1) posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień,
2) posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia, lub przedstawią pisemne zobowiązanie innych podmiotów do udostępnienia potencjału technicznego i osób zdolnych do wykonania zamówienia;
3) znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
4) nie podlegają wykluczeniu z postępowania o udzielenie zamówienia.

Ocena spełniania warunków udziału w postępowaniu zostanie dokonana na podstawie dokumentów złożonych przez Wykonawcę, na zasadzie SPEŁNIA/NIE SPEŁNIA.

2. Każdy z wykonawców ma obowiązek złożyć następujące oświadczenia i dokumenty potwierdzające spełnienie warunków udziału w postępowaniu:
   1) **Oświadczenie wykonawcy**, według wzoru, stanowiącego **załącznik nr 2** do niniejszej siwz o spełnianiu warunków określonych w art. 22 ust. 1 ustawy,
      W przypadku składania oferty wspólnej ww. oświadczenie składa pełnomocnik w imieniu wykonawców składających ofertę wspólną.
   2) **Aktualny odpis z właściwego rejestru** albo **aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej** (*jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności),* wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
      W przypadku składania oferty wspólnej ww. dokument składa każdy z wykonawców składających ofertę wspólną.

3. Ponadto wykonawcy mają dołączyć do oferty następujące dokumenty:
   1) ofertę cenową zgodnie z Rozdziałem I pkt 3 siwz;
      W przypadku składania oferty wspólnej należy złożyć jeden dokument
   2) odpowiednie pełnomocnictwa;
      Tylko w sytuacjach określonych w Rozdziale I pkt 5 zdanie 2 siwz lub w przypadku składania oferty wspólnej (Rozdział III pkt 1 siwz)
   3) oświadczenie według wzoru stanowiącego załącznik nr 1 do siwz wskazujące cześć zamówienia, której wykonanie wykonawca powierzy podwykonawcom (jeżeli wykonawca przewiduje udział podwykonawców);
      W przypadku składania oferty wspólnej należy złożyć jeden dokument
   4) opis parametrów technicznych oferowanego przedmiotu zamówienia, w celu ustalenia zgodności z opisem przedmiotu określonym w siwz, sporządzony zgodnie ze wzorem stanowiącym załącznik nr 4-6 do siwz, w zależności na którą grupę wykonawca składa swoją ofertę.
      W przypadku składania oferty wspólnej należy złożyć jeden dokument

4. Zamawiający wezwie wykonawców, którzy w określonym terminie nie złożą oświadczeń lub dokumentów, o których mowa w art. 25 ust. 1 ustawy, lub którzy nie złożyli pełnomocnictw, albo którzy złożyli wymagane przez zamawiającego oświadczenia i dokumenty, o których mowa w art. 25 ust. 1, zawierające błędy lub którzy złożyli wadliwe pełnomocnictwa, do ich złożenia w wyznaczonym terminie, chyba że mimo ich złożenia oferta wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

Złożone na wezwanie zamawiającego oświadczenia i dokumenty powinny potwierdzać spełnianie przez wykonawcę warunków udziału w postępowaniu oraz spełnianie przez oferowane dostawy wymagań określonych przez zamawiającego, nie później niż w dniu, w którym upłynął termin składania ofert.

5. W przypadku załączenia do oferty innych dokumentów niż wymagane przez zamawiającego (np. materiałów reklamowych i informacyjnych) zaleca się aby stanowiły one odrębną część, niezłączoną z ofertą w sposób trwały. Dokumenty takie nie będą podlegały ocenie przez zamawiającego.

ROZDZIAŁ VI Wykonawcy zagraniczni

1. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu, o którym mowa w rozdziale V pkt 2 ppkt 2) siwz składa dokument lub dokumenty, wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
   -nie otwarto jego likwidacji ani nie ogłoszono upadłości,
2. Dokumenty, o których mowa w pkt 1, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
3. Jeżeli w kraju pochodzenia osoby lub w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów o których mowa w pkt 1 zastępuje się je dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio kraju pochodzenia osoby lub kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania. Przepis pkt 2 stosuje się odpowiednio.

ROZDZIAŁ VII Termin wykonania zamówienia i gwarancja

1. Termin wykonania zamówienia nie może być dłuższy niż 14 dni kalendarzowych od dnia podpisania umowy.
2. Wymagany przez zamawiającego okres gwarancji w grupie III – 36 miesięcy od dnia dostarczenia sprzętu.

ROZDZIAŁ VIII Wadium

1. Wadium należy wnieść w wysokości :
   1) kwota wadium dla grupy 1 : **2 200 zł** (dwa tysiące dwieście złotych brutto)
   2) kwota wadium dla grupy 2 : **1 600 zł** (tysiąc sześćset złotych brutto)
   3) kwota wadium dla grupy 3 : **2 400 zł** (dwa tysiące czterysta złotych brutto)

   w terminie do dnia **16.02.2009 r.** do godz. **10 30**.

   Decyduje data wpływu środków do zamawiającego.
2. Wadium może być wnoszone:
   1) w pieniądzu – przelewem na konto depozytowe Urzędu Miasta Szczecin Bank PKO S.A. II O/Szczecin Nr 16 1240 3927 1111 0000 4099 5290.

2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej (z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym), gwarancjach bankowych, gwarancjach ubezpieczeniowych, poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2) ustawy z dnia 9 listopada 2000r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości - w kasie wewnętrznej Urzędu Miasta Szczecin, pok. nr 126, w poniedziałki w godz. 9:45 – 16:00, a w pozostałe dni tygodnia w godz. 9:15 – 14:00

3. Wykonawca, którego oferta została wybrana, traci wadium wraz z odsetkami na rzecz zamawiającego w przypadku gdy:
   1) odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie,
   2) zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie wykonawcy,
   3) **w odpowiedzi na wezwanie, o którym mowa w Rozdziale V pkt 4 niniejszej siwz, nie złożył dokumentów lub oświadczeń, o których mowa w art. 25 ust. 1, lub pełnomocnictw. Zamawiający zwróci wadium jeśli wykonawca udowodni, że nastąpiło to z przyczyn nie leżących po jego stronie.**
4. W przypadku, gdy wykonawca wnosi wadium w formie gwarancji bankowej lub gwarancji ubezpieczeniowej z treści tych gwarancji musi w szczególności jednoznacznie wynikać:
   1) zobowiązanie gwaranta (banku, zakładu ubezpieczeń) do zapłaty całej kwoty wadium **nieodwołalnie i bezwarunkowo** na pierwsze żądanie zamawiającego (beneficjenta gwarancji) zawierające oświadczenie, że zaistniały okoliczności, o których mowa w pkt 3 bez potwierdzania tych okoliczności,
   2) termin obowiązywania gwarancji, który nie może być krótszy niż termin związania ofertą,
   3) miejsce i termin zwrotu gwarancji.
5. Wadium może być wniesione w jednej lub kilku formach.
6. Wykonawca, który nie zabezpieczy swojej oferty akceptowaną formą wadium zostanie przez zamawiającego wykluczony a oferta uznana za odrzuconą.
7. W ofercie należy wpisać nr konta, na który zamawiający będzie mógł zwrócić wadium lub do oferty załączyć upoważnienie dla osoby, której zamawiający będzie mógł zwrócić wadium.
8. Wadium wniesione w pieniądzu zamawiający przechowa na rachunku bankowym.
9. Dyspozycję w zakresie wypłaty wadium wpłaconego w formie pieniężnej, dla wykonawców, których oferty nie zostaną wybrane, zamawiający przekaże do właściwego oddziału banku wykonawcy niezwłocznie po podpisaniu umowy przez wykonawcę, którego oferta została wybrana, lecz nie później niż następnego dnia po zakończeniu związania ofertą.
10. Dyspozycję w zakresie wypłaty wadium wpłaconego w formie pieniężnej, dla wykonawcy, którego oferta zostanie wybrana, zamawiający przekaże do właściwego oddziału banku wykonawcy niezwłocznie po podpisaniu umowy.
11. Zamawiający, z zastrzeżeniem pkt 3 ppkt 3) Rozdziału VIII siwz zwróci wadium niezwłocznie po zgłoszeniu pisemnego wniosku przez wykonawcę:
    1) który wycofał ofertę przed upływem terminu składania ofert,

2) który został wykluczony z postępowania,
3) którego oferta została odrzucona.

12. Jeżeli wadium zostanie wniesione w pieniądzu zamawiający zwróci je wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane pomniejszonym o koszty prowadzenia rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek wykonawcy.

ROZDZIAŁ IX Wyjaśnienia treści SIWZ i jej modyfikacja oraz sposób porozumiewania się wykonawców z zamawiającym

1. Zamawiający urzęduje w następujących dniach (pracujących) i godzinach:
   poniedziałki – od godz. 9:00 do godz. 17:00
   wtorki – piątki – od godz. 7:30 do godz. 15:30
2. Oświadczenia, wnioski, zawiadomienia oraz informacje zamawiający i wykonawca przekazują **pisemnie**, z zastrzeżeniem pkt 3.
3. Zamawiający dopuszcza porozumiewanie się za pomocą **faksu**, przy przekazywaniu następujących dokumentów:
   1) pytania i wyjaśnienia dotyczące treści siwz,
   2) modyfikacje treści siwz,
   3) wniosek wykonawcy o przekazanie informacji z otwarcia ofert, o których mowa w art. 86 ustawy oraz odpowiedź zamawiającego
   4) wniosek o wyjaśnienie i wyjaśnienie treści oferty,
   5) wniosek o wyjaśnienie i wyjaśnienia dotyczące oświadczeń i dokumentów, o których mowa w art. 25 ust. 1 ustawy,
   6) wezwanie kierowane do wykonawców na podstawie art. 26 ust. 3 ustawy,
   7) informacja o poprawieniu oczywistych omyłek pisarskich oraz oczywistych omyłek rachunkowych,
   8) informacje o poprawieniu innych omyłek polegających na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujących istotnych zmian w treści oferty
   9) oświadczenie wykonawcy w kwestii wyrażenia zgody na poprawienie innych omyłek polegających na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujących istotnych zmian w treści oferty
   10) wniosek zamawiającego o wyrażenie zgody na przedłużenie terminu związania ofertą oraz odpowiedź wykonawcy,
   11) oświadczenie wykonawcy o przedłużeniu terminu związania ofertą,
   12) zawiadomienie o wyborze najkorzystniejszej oferty, o wykonawcach, którzy zostali z postępowania wykluczeni i wykonawcach, których oferty zostały odrzucone,
   13) zawiadomienie o unieważnieniu postępowania,
   14) informacje i zawiadomienia kierowane do wykonawców na podstawie art. 181 ustawy.
4. Jeżeli zamawiający lub wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje faksem, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
5. Korespondencja przesłana za pomocą faksu po godzinach urzędowania zostanie zarejestrowana w następnym dniu pracy zamawiającego i uznana za wniesioną z datą tego dnia.

6. Postępowanie odbywa się w języku polskim w związku z czym wszelkie pisma, dokumenty, oświadczenia itp. składane w trakcie postępowania między zamawiającym a wykonawcami muszą być sporządzone w języku polskim.
7. Adres do korespondencji jest zamieszczony na pierwszej stronie niniejszej siwz. Zamawiający wymaga, aby wszelkie pisma związane z postępowaniem były kierowane wyłącznie na ten adres.
8. Zamawiający nie zamierza zwoływać zebrania wykonawców.
9. Osobą uprawnioną do bezpośredniego kontaktowania się z wykonawcami jest **p. Mirella Wołłejszo** tel. (091) 42-45-101 w godz. 10.00-14.00, fax (091) 42-45-104 (czynny całą dobę).
10. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści siwz. Zamawiający udzieli niezwłocznie wyjaśnień, chyba że prośba o wyjaśnienie treści siwz wpłynie do niego na mniej niż 6 dni przed terminem składania ofert.
11. Treść zapytań wraz z wyjaśnieniami Zamawiający przekazuje wykonawcom, którym przekazał siwz bez ujawniania źródła zapytania oraz udostępnia na stronie internetowej.
12. W uzasadnionych przypadkach zamawiający może przed upływem terminu składania ofert zmienić treść specyfikacji istotnych warunków zamówienia. Dokonaną zmianę specyfikacji zamawiający przekazuje niezwłocznie wszystkim wykonawcom, którym przekazano specyfikację istotnych warunków zamówienia, a jeżeli specyfikacja jest udostępniana na stronie internetowej, zamieszcza ją także na tej stronie.
13. Jeżeli w wyniku zmiany treści specyfikacji istotnych warunków zamówienia nieprowadzącej do zmiany treści ogłoszenia o zamówieniu jest niezbędny dodatkowy czas na wprowadzenie zmian w ofertach, zamawiający przedłuża termin składania ofert i informuje o tym wykonawców, którym przekazano specyfikację istotnych warunków zamówienia, oraz na stronie internetowej, jeżeli specyfikacja istotnych warunków zamówienia jest udostępniana na tej stronie.

ROZDZIAŁ X Sposób obliczenia ceny oferty

1. Cena powinna obejmować wszystkie pozycje zamówienia, podatek VAT oraz wszystkie inne pozostałe koszty realizacji zamówienia, w szczególności koszty dostawy do siedziby zamawiającego.
2. Wykonawca musi podać ceny oddzielnie na każdą część zamówienia, na którą składa ofertę.
3. Rozliczenia między zamawiającym a wykonawcą będą prowadzone w walucie PLN.
4. Cena musi być wyrażona w złotych polskich niezależnie od wchodzących w jej skład elementów. Tak obliczona cena będzie brana pod uwagę przez komisję przetargową w trakcie wyboru najkorzystniejszej oferty.
5. Zastosowanie przez wykonawcę stawki podatku VAT od towarów i usług niezgodnej z obowiązującymi przepisami spowoduje odrzucenie oferty.
6. Błąd w obliczeniu ceny, którego nie można poprawić na podstawie art. 87 ust. 2 pkt. 2 Prawa zamówień publicznych spowoduje odrzucenie oferty.

ROZDZIAŁ XI Składanie i otwarcie ofert

1. Ofertę należy złożyć w Biurze ds. Zamówień Publicznych, pok. Nr 397, w terminie do dnia **16.02.2009 r.**, do godz. **10 30**.
2. Za termin złożenia oferty uważa się termin jej wpłynięcia do zamawiającego.
3. Wykonawca otrzyma pisemne potwierdzenie złożenia oferty.
4. Oferty będą podlegać rejestracji przez zamawiającego. Każda przyjęta oferta zostanie opatrzona adnotacją określającą dokładny termin przyjęcia oferty tzn. datę kalendarzową oraz godzinę i minutę, w której została przyjęta. Do czasu otwarcia ofert, będą one przechowywane w sposób gwarantujący ich nienaruszalność.
5. Otwarcie ofert odbędzie się w dn. **16.02.2009 r.**, o godz. **11 00** w Urzędzie Miasta Szczecin, w Biurze ds. Zamówień Publicznych, pok. Nr 397
6. Postępowanie o udzielenie zamówienia jest przeprowadzane przez komisję przetargową powołaną Zarządzeniem Prezydenta Miasta Szczecin Nr 27/09 z dnia 30 stycznia 2009 r.
7. Postępowanie toczyć się będzie z podziałem na część: jawną i niejawną.
8. Zamawiający bezpośrednio przed otwarciem ofert poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia. Następnie zamawiający otworzy koperty z ofertami i ogłosi nazwę (firmę) i adres (siedzibę) wykonawcy, którego oferta jest otwierana, a także informacje dotyczące ceny oferty, terminu wykonania zamówienia, okresu gwarancji – zawartych w ofercie.
9. Informacje, o których mowa w pkt 8 zamawiający przekaże niezwłocznie wykonawcom, którzy nie byli obecni przy otwarciu ofert, na ich wniosek.

ROZDZIAŁ XII Wybór oferty najkorzystniejszej

1. Jedynym kryterium oceny ofert jest cena.
2. Sposób przyznania punktów w kryterium cena:

$$\frac{\text{cena najniższa}}{\text{cena oferty ocenianej}} \times 100 \text{ pkt} \times \text{znaczenie kryterium } 100\ \%$$

Zamawiający dokona oceny ofert oddzielnie dla każdej z grup.

3. Wykonawca pozostaje związany ofertą przez okres 30 dni.
4. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
5. Zamawiający dokona badania ofert w celu stwierdzenia, czy wykonawcy nie podlegają wykluczeniu. W przypadku wykluczenia wykonawcy zamawiający odrzuci jego ofertę. Następnie zamawiający dokona oceny, czy oferty wykonawców nie wykluczonych z postępowania nie podlegają odrzuceniu.
6. W toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert i dokumentów potwierdzających spełnianie warunków udziału w postępowaniu.

7. Zamawiający poprawi w tekście oferty oczywiste omyłki pisarskie oraz oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonywanych poprawek niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.
8. Zamawiający poprawi w tekście oferty inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujące istotnych zmian w treści oferty niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.
9. Jeżeli oferta zawierać będzie rażąco niską cenę w stosunku do przedmiotu zamówienia, zamawiający zwróci się w formie pisemnej do wykonawcy o udzielenie w określonym terminie wyjaśnień dotyczących elementów oferty mających wpływ na wysokość ceny.
10. Zamawiający odrzuci ofertę, jeżeli:
    1) jest niezgodna z ustawą,
    2) jej treść nie odpowiada treści specyfikacji istotnych warunków zamówienia, z zastrzeżeniem art. 87 ust. 2 pkt 3;
    3) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji,
    4) zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia,
    5) została złożona przez wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia lub niezaproszonego do składania ofert,
    6) zawiera błędy w obliczeniu ceny;
    7) wykonawca w terminie 3 dni od dnia doręczenia zawiadomienia nie zgodził się na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3;
    8) jest nieważna na podstawie odrębnych przepisów.
11. Oferty nie odrzucone zostaną poddane procedurze oceny zgodnie z kryteriami oceny ofert określonymi w siwz.
12. Zamawiający wybierze ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w siwz.
13. Niezwłocznie po wyborze najkorzystniejszej oferty zamawiający zawiadomi wykonawców, którzy złożyli oferty o:
    1) wyborze najkorzystniejszej oferty, podając nazwę (firmę) i adres tego wykonawcy, którego ofertę wybrano, oraz uzasadnienie jej wyboru, a także nazwy (firmy), siedziby i adresy wykonawców, którzy złożyli oferty wraz ze streszczeniem oceny i porównania złożonych ofert zawierającym punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,
    2) wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne,
    3) wykonawcach, którzy zostali wykluczeni z postępowania, podając uzasadnienie faktyczne i prawne
14. W przypadku wystąpienia przesłanek, o których mowa w art. 93 ust. 1 ustawy zamawiający unieważnia postępowanie.
15. O unieważnieniu postępowania zamawiający zawiadomi równocześnie wszystkich wykonawców, którzy:

1) ubiegali się o udzielenie zamówienia, - w przypadku unieważnienia postępowania przed upływem terminu składania ofert,
2) złożyli oferty - w przypadku unieważnienia postępowania po upływie terminu składania ofert

- podając uzasadnienie faktyczne i prawne.

16. Zamawiający zwróci wykonawcom, których oferty nie zostały wybrane, na ich wniosek, złożone przez nich plany, projekty, rysunki, modele, próbki, wzory, programy komputerowe oraz inne podobne materiały.

ROZDZIAŁ XIII Zawarcie umowy

1. **Informacje o formalnościach, jakie powinny być spełnione w celu zawarcia umowy**.
   1) Wykonawca, którego oferta została wybrana zobowiązany jest skontaktować się z zamawiającym w terminie 7 dni od daty przekazania zawiadomienia o wyborze oferty i uzgodnić termin podpisania umowy.
   2) Wykonawca ma obowiązek zawrzeć umowę zgodnie ze wzorem umowy stanowiącym **załącznik nr 3a lub 3b** do niniejszej siwz **w zależności od grupy na którą zawierana jest umowa**.
   3) Zawarta umowa będzie jawna i będzie podlegała udostępnianiu na zasadach określonych w przepisach o dostępie do informacji publicznej (art. 139 ust. 3 ustawy).
2. Termin i miejsce zawarcia umowy.
   1) Umowa zostanie zawarta w siedzibie zamawiającego, nie wcześniej niż w 8 dniu od daty przekazania zawiadomienia o wyborze oferty.
   2) Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w pkt. 2 ppkt 1, jeżeli w postępowaniu o udzielenie zamówienia została złożona tylko jedna oferta.

ROZDZIAŁ XIV Pouczenie o środkach ochrony prawnej

1. Wykonawcom, których interes prawny w uzyskaniu zamówienia doznał lub może doznać uszczerbku w wyniku naruszenia przez zamawiającego przepisów ustawy, przysługują środki ochrony prawnej przewidziane w dziale VI ustawy: protest odwołanie i skarga.
2. Wobec czynności podjętych przez zamawiającego w toku postępowania oraz w przypadku zaniechania przez zamawiającego czynności, do której jest obowiązany na podstawie ustawy, Wykonawca ma prawo wnieść protest w terminach określonych w ustawie.
3. Wniesienie protestu jest dopuszczalne tylko przed zawarciem umowy.
4. Zamawiający odrzuca protest wniesiony po terminie, wniesiony przez podmiot nieuprawniony lub protest niedopuszczalny na podstawie art. 181 ust. 6.
5. Protest powinien wskazywać oprotestowaną czynność lub zaniechanie zamawiającego, a także zawierać żądanie, zwięzłe przytoczenie zarzutów oraz okoliczności faktycznych i prawnych uzasadniających wniesienie protestu.
6. Odwołanie przysługuje wyłącznie od rozstrzygnięcia protestu dotyczącego:
   1) opisu sposobu oceny spełniania warunków udziału w postępowaniu;
   2) wykluczenia wykonawcy z postępowania o udzielenie zamówienia;

3) odrzucenia oferty.

7. Odwołanie wnosi się do Prezesa Urzędu w terminie **5 dni** od dnia doręczenia rozstrzygnięcia protestu lub upływu terminu do rozstrzygnięcia protestu, jednocześnie przekazując jego kopię zamawiającemu. Złożenie odwołania w placówce pocztowej operatora publicznego jest równoznaczne z wniesieniem do Prezesa Urzędu.
8. Na wyrok **Krajowej Izby Odwoławczej** oraz postanowienia **Krajowej Izby Odwoławczej** kończące postępowanie odwoławcze przysługuje skarga do sądu.

ROZDZIAŁ XV Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa oprogramowania antywirusowego dla Urzędu Miasta Szczecin. Zakres zamówienia obejmuje następujące grupy:

I. Grupa 1

Nazwa i kod Wspólnego Słownika Zamówień (CPV: 48.76.10.00-0)

Zaawansowane technologicznie zabezpieczenie antywirusowe i antyspyware dla 1000 stacji roboczych i 50 serwerów plików, zawierające centralną administrację. Obecnie Zamawiający posiada 1000 licencji F-Secure Anti-Virus Client Security i 50 licencji Nod32 Mix wraz z konsolą administracyjną.

1. Wymagania dotyczące oprogramowania antywirusowego :

a. ochrona 1000 stacji roboczych Windows 2000/XP/Vista 32 i Vista 64.
b. ochrona 50 serwerów Windows 2000/2003 32 i 64 bity /2008 32 i 64 bity oraz Linux Red Hat, SUSE, Debian, Ubuntu.
c. ochrona całego systemu monitorowana i zarządzana z pojedynczej konsoli, zarówno po stronie administratora jak i użytkownika końcowego
d. możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.
e. polski interfejs użytkownika
f. ochrona antywirusowa realizowana na trzech poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki danych i monitora poczty elektronicznej,
g. Wbudowana technologia do ochrony przed rootkitami
h. oddzielny zintegrowany silnik antyspyware
i. aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu,
j. możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta,
k. aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym
l. brak konieczności restartu komputerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów
m. heurystyczna technologia do wykrywania nowych, nieznanych wirusów,

n. wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan"
o. Automatyczna, przyrostowa aktualizacja baz wirusów i innych zagrożeń, bez konieczności pobierania całej bazy.
p. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy
q. obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej : ZIP ARJ TAR TGZ CAB RAR
r. automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa,
s. automatyczne uruchamianie procedur naprawczych,
t. oprogramowanie zapewnia w procesie skanowania ręcznego i automatycznego przeskanowanie dowolnego celu pod względem wirusów, spyware, rootkitow, riskware
u. Możliwość skanowania dysków sieciowych i dysków przenośnych
v. program posiada kwarantanne wirusów, spyware oraz riskware
w. program pozwala z interfejsu graficznego użytkownika wysłać próbkę wirusa bezpośrednio do laboratorium antywirusowego producenta
x. automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona
y. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook,
z. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji
aa. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie
bb. ochrona przeglądarki internetowej, w tym : blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), analiza uruchamianych skryptów ActiveX i pobieranych plików
cc. kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną
dd. osobista zapora ogniowa stacji roboczych (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych, z możliwością automatycznego ustawiania profilu w zależności od lokalizacji w której znajduje się stacja robocza
ee. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania

2. Wymagania dotyczące systemu centralnego zarządzania i raportowania :

a. Możliwość instalacji serwera centralnego zarządzania na serwerach Windows 2000/2003/2008.
b. Możliwość instalacji konsoli centralnego zarządzania na jednej z następujących platform Windows 2000/XP/2003/Vista/2008.
c. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI)
d. Możliwość wykonania bezpośredniej instalacji zdalnej nienadzorowanej

e. narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję,
f. pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem),
g. pełne centralne zarządzanie dla środowisk Windows 2000/2003/XP/Vista, Linux
h. scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta,
i. administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa
j. centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy,
k. możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów)
l. tworzenie grup , zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach,
m. możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych i w celu uniemożliwienia ich modyfikacji przez użytkowników,
n. możliwość wyłączenia blokady zmiany ustawień dla użytkownika z prawami administratora
o. serwer zarządzający związany z konsolą zarządzającą musi mieć funkcję przesyłania aktualizacji do klientów z możliwością ustawienia harmonogramu lub częstotliwości aktualizacji,
p. możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający,
q. możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji,
r. umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe,
s. codzienne automatyczne aktualizacje uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących.
t. możliwość automatycznego raportowania do pliku w formacie HTML
u. możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich,
v. możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”,
w. możliwość lokalnego zarządzania wszystkimi ustawieniami programu klienta,
x. program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa,
y. program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe,
z. program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy),

aa. program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów,
bb. zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania

3. Wykonawca musi przedłożyć informację o proponowanych produktach w formie tabeli zawierającej w/w wymagania techniczne. (załącznik nr 4 do SIWZ).

II. Grupa 2

Nazwa i kod Wspólnego Słownika Zamówień (CPV: 48.21.95.00-1)

1. Aktualizacja licencji F-Secure Messaging Security Server na okres 3 lat do urządzenia F-secure Messaging Security Gateway X200 Appliance, które posiada zamawiający - 1000 szt.

albo:

nowe urządzenie do kompleksowego systemu ochrony poczty elektronicznej z 1000 licencji na okres 3 lat od dnia odbioru końcowego spełniających poniższe wymagania :

a. System powinien zapewniać ochronę przed zagrożeniami związanymi z przesyłaniem poczty elektronicznej (wirusy, spam, phishing, niedozwolone treści, etc.)
b. Moduł detekcji spamu powinien bazować na metodzie zaawansowanej analizy statystycznej, która wyklucza konieczność ręcznego tworzenia reguł w razie pojawienia się nowych technik omijania filtrów antyspamowych
c. System w momencie dostarczenia lub po odtworzeniu powninien zawierać zestaw predefinowanych reguł i polityk dla wszystkich modułów filtrujących: AV, antispam, kontrola treści
d. System w momencie dostarczenia lub po odtworzeniu powninien zawierać zestaw predefiniowanych raportów
e. System powinien zapewniać ochronę przeciwko atakom typu Odmowa dostępu do usług (Denial Of Service) oraz logować i zapobiegać enumeracji kont użytkowników chronionej domeny pocztowej (Directory Harvesting Attack)
f. Zarządzanie lokalne i zdalne systemem powinno być możliwe przy użyciu bezpiecznego połączenia https przez przeglądarkę internetową oraz poprzez protokół ssh
g. System powinien pracować jako brama smtp i być niezależnym od rodzaju stosowanego, chronionego serwera poczty
h. System powinien zapewniać możliwość szyfrowania przesyłek za pomocą protokołu Transport Layer Security w warstwie sieciowej
i. System powinien umożliwiać korzystanie z zewnętrznych serwerów RBL
j. System powinien zapewniać wsparcie dla standardu Sender Policy Framework
k. System pownien zapewnić możliwość zdefiniowania osobnych tras przesyłania poczty dla ruchu przychodzącego i wychodzącego w oparciu o statyczne wpisy adresów serwerów, smart hosta lub rekordy MX serwerów dns

l. System powinien zapewniać inteligentne rozpoznawanie typów analizowanych załączników
m. Ochrona antywirusowa powinna być realizowana przy pomocy minimum trzech niezależnych silników skanujących
n. Aktualizacje sygnatur modułu antywirusowego powinny być dostępne nie rzadziej niż raz na dobę
o. System powinien zapewniać możliwość tworzenia kilku polityk ochrony antywirusowej przydzielanych w oparciu o: adresy IP serwera nadawcy, adres email nadawcy/odbiorcy wiadomości
p. Możliwość definiowania różnych sposobów postępowania z zainfekowanymi wiadomościami w zależności od rodzaju wykrytego wirusa
q. Możliwość określenia postępowania z zabezpieczonymi wiadomościami (załączniki chronione hasłem, podpisane wiadomości, etc.)
r. System powinien posiadać lokalną kwarantannę dla zainfekowanych wiadomości
s. System powinien zapewniać automatyczną ocenę reputacji źródła przesyłanego mail'a (na podstawie ilości połączeń, procentowej ilości maili z wirusami, procentowej ilości wiadomości zakwalifikowanych jako spam)
t. System powinien posiadać moduł antyspamowy zapewniający analizę statystyczną wiadomości na podstawie minimum 200.000 atrybutów maila
u. Możliwość definiowania reguł antyspamowych na poziomie całego urządzenia, grup użytkowników oraz pojedynczych użytkowników
v. Listy użytkowników definiowane lokalnie, możliwość importu użytkowników z serwerów: Active Directory, LDAP, MS Exchange, Lotus Domino oraz plików (tekstowe, csv)
w. System zapewni możliwość zarządzania użytkownikom końcowym wiadomościami trafiającymi do ich personalnej kwarantanny
x. Możliwość określania poziomu dostępu i akcji możliwych do wykonania w obrębie kwarantanny dla różnych użytkowników/grup użytkowników
y. Kwarantanna końcowego użytkownika musi wykorzystywać istniejące oprogramowanie klientów poczty elektronicznej lub przeglądarki internetowej bez konieczności instalowania dodatkowego oprogramowania na stacjach roboczych oraz działać w oparciu o bezpieczną komunikację https
z. System powinien zapewniać możliwość opcjonalnego uwierzytelniania użytkownika w celu zmian parametrów własnego folderu kwarantanny
aa. System zapewni możliwość definiowania list zaufanych i blokowanych nadawców przez użytkowników końcowych
bb. Możliwość definiowania wyglądu kwarantanny końcowego użytkownika zarówno co do jej szaty graficznej (np. możliwość umieszczenia znaku firmowego) jak i treści komunikatów
cc. System powinien zapewniać możliwość tworzenia własnych reguł filtrowania treści w oparciu o: adresy IP nadawców odbiorców, adresy email, typ i rozmiar załącznika, ilość załączników, treść maila, pola nagłówka wiadomości, treść załączników
dd. Rozbudowany system raportowania zapewniający dostęp do minimum 45 różnych rodzajów graficznych raportów

ee. Możliwość okresowej publikacji wybranych raportów jako strony WWW, przy pomocy wysyłanych automatycznie wiadomości email oraz jako pliki xml

ff. Logowanie na lokalnym dysku twardym lub zewnętrznym serwerze syslog zdarzeń podejmowanych przez filtry oraz zdarzeń dotyczących komunikacji smtp

gg. Możliwość definiowania i przeglądania wielu katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych

hh. Dla wszystkich stworzonych folderów kwarantanny system zapewni możliwość ustawienia maksymalnego czasu przechowywania wiadomości a po jego upływie automatycznie je usunie

ii. System zapewni administratorowi wskazanie folderu/ów, z których wysyłany będzie skrót informacji o wiadomościach do personalnej kwarantanny użytkownika

jj. System powinien umożliwiać następujące operacje na wiadomościach przechowywanych w obszarze kwarantanny: usunięcie wiadomości, przesłanie do odbiorcy, przeniesienie do innego folderu

kk. Urządzenie powinno zapewnić możliwość zgłoszenia przypadków złej klasyfikacji wiadomości do producenta systemu na poziomie kwarantanny administratora oraz personalnej kwarantanny użytkownika końcowego

ll. Możliwość zapisu i odtworzenia konfiguracji

mm. System powinien zapewniać możliwość zdefiniowania wielu administratorów o zróżnicowanych uprawnieniach

nn. System powinien zapewniać automatyczną aktualizację sygnatur antywirusowych, silników skanujących, modułów systemu antyspamowego, oprogramowania i systemu operacyjnego z serwera producenta oraz poprawki dotyczące agenta MTA

oo. Wszystkie aktualizacje powinny być pobierane z jednego miejsca a system komunikować się ze źródłem aktualizacji z częstotliwością narzuconą przez administratora systemu

pp. System zapewni śledzenie historii wykonywania aktualizacji

qq. Producent powinien zapewnić możliwość zakupu aktualizacji systemu jednorazowo na okres roku, dwóch lub trzech lat

2. Wykonawca musi przedłożyć informację o proponowanych produktach w formie tabeli zawierającej w/w wymagania techniczne. (załącznik nr 5 do SIWZ).

III. Grupa 3

Nazwa i kod Wspólnego Słownika Zamówień (CPV: 48.20.00.00-0)

Rozwiązanie sprzętowe do zapewnienia Bezpieczeństwa Brzegowego Sieci zawierającego Fitr witryn WWW oparty na kategoriach blokujących dostęp po URL oraz możliwość blokowania komunikatorów i ruchu P2P.
Wymagania techniczne kompleksowego systemu zabezpieczeń :

1. Typ urządzenia

   a. Dwa urządzenia typu UTM, zapewniające funkcjonalności: Firewall, Koncentrator IPSec VPN, ochrona przed wirusami, spyware, sonda IPS, filtrowanie treści, działające w klastrze wysokiej dostępności Active-Passive z synchronizacją sesji.
2. Specyfikacja fizyczna urządzenia
   a. Dedykowane rozwiązanie sprzętowe
   b. Obudowa nie większa niż 2U przeznaczona do montażu w szafie RACK
   c. Redundantne zasilacze i wentylatory z możliwą wymianą hot-swap
   d. Pamięć RAM: minimum 1 GB
   e. Pamięć FLASH: minimum 512 MB Compact Flash
   f. Procesor wielordzeniowy
   g. Nie mniej niż 8 portów GigabitEthernet
   h. 1 interfejs GigabitEthernet dedykowany do połączenia dwóch jednakowych urządzeń w klaster HA
   i. 1 interfejs konsoli
3. Wydajność urządzeń pracujących w klastrze HA Active-Passive
   a. Obsługa nielimitowanej ilości hostów w sieci chronionej
   b. Przepustowość zapory sieciowej przy pracy w trybie Statefull Packet Inspection, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 5 Gbps
   c. Przepustowość zapory sieciowej pracującej jako sonda IPS, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 2,3 Gbps
   d. Przepustowość zapory sieciowej przy pracy w trybie Deep Packet Inspection, przy włączonych wszystkich usługach filtrowania i skanowania: nie mniejsza niż 1,5 Gbps
   e. Przepustowość zintegrowanego z zaporą sieciową koncentratora połączeń IPSec VPN AES/3DES mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 2,5 Gbps
   f. Maksymalna ilość jednocześnie obsługiwanych sesji: nie mniej niż 750000
   g. Obsługa nie mniej niż 20000 nowych sesji na sekundę
   h. Ochrona przed atakami DoS i DDoS
4. Funkcjonalności urządzeń w zakresie konfiguracji połączeń IPSec VPN
   a. Minimalna ilość jednocześnie obsługiwanych połączeń IPSec VPN: 6000
   b. Minimalna ilość klientów IPSec VPN w cenie urządzenia: 2000
   c. Wspierane mechanizmy uwierzytelniania i szyfrowania: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1
   d. Wspierane mechanizmy wymiany kluczy: IKE, IKEv2, Manual Key, PKI (X.509)
   e. Wsparcie certyfikatów: Verisign, RSA Keon, Entrust, Microsoft CA dla połączeń site-to-site pomiędzy urządzeniami
   f. Obsługa funkcjonalności: L2TP IPSec, DHCP over VPN, redundantna brama zdalna w przypadku połączeń site-site VPN
5. Sieciowe funkcjonalności urządzeń
   a. Możliwość pracy jako Router, Bridge L2 lub w trybie transparentnym
   b. Obsługa nie mniej niż 256 sieci VLAN działających zgodnie ze standardem 802.1Q
   c. Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP
   d. Możliwość przesyłania komunikatów DHCP pomiędzy różnymi strefami
   e. Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many, PAT
   f. Możliwość scentralizowanego zarządzania nie mniej niż 128 punktami dostępowymi, wsparcie dla standardów 802.11 b/g, WEP, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS, IPSec over WLAN

g. Możliwość kreowania reguł routingu statycznego
h. Wsparcie dynamicznych protokołów routingu: RIP v1/v2, OSPF i wsparcie dla routowania transmisji multicast
i. Wsparcie funkcjonalności QoS: tagowanie/mapowanie 802.1p, DSCP, możliwość ustawienia przynajmniej 100 reguł określających maksymalne i gwarantowane pasmo
j. Możliwość skonfigurowania przynajmniej 2 łączy WAN, działających w trybie redundantnym lub umożliwiających równoważenie obciążeń dla ruchu wychodzącego.
k. Możliwość konfiguracji monitorowania pracy łączy WAN w oparciu o połączenia TCP i ICMP i reguł przełączenia ruchu z łącza podstawowego na łącze redundantne
l. Możliwość konfiguracji reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej
m. Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, pełna kompatybilność z większością urządzeń i serwerów VoIP

6. Funkcjonalności urządzeń w zakresie uwierzytelniania użytkowników
   a. Lokalna baza użytkowników umożliwiająca wykreowanie nie mniej niż 2500 kont
   b. Uwierzytelnianie użytkowników w oparciu o: XAUTH/RADIUS, Active Directory, SSO, LDAP, lokalna baza użytkowników
7. Funkcjonalności urządzeń w zakresie zarządzania i wysokiej dostępności
   a. Możliwość zarządzania urządzeniem poprzez: HTTP, HTTPS, CLI (SSH, konsola), SNMP v2
   b. Praca w klastrze wysokiej dostępności w trybie Active – Passive z synchronizacją sesji
8. Funkcjonalności urządzeń w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection
   a. Możliwość kreowania stref bezpieczeństwa przydzielanych do danych interfejsów zarówno fizycznych, jak i wirtualnych (możliwość przypisania więcej niż jednego interfejsu do pojedynczej strefy bezpieczeństwa)
   b. Możliwość indywidualnej konfiguracji usług bezpieczeństwa dla każdej ze stref
   c. Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do zadanej strefy, w określonych przedziałach czasu, z uwzględnieniem użytkowników, dla których reguła ma być aktywna
   d. Możliwość włączania i wyłączania reguł Firewall i NAT bez konieczności ich usuwania
   e. Wymagane jest, aby na urządzeniach uruchomione były następujące usługi w subskrypcji na 3 lata:
      i. Sieciowa ochrona antywirusowa zapewniająca skanowanie ruchu na protokołach HTTP, FTP, POP3, SMTP, IMAP, ruch TCP oraz NetBios. Filtr antywirusowy powinien zapewniać skanowanie załączników poczty elektronicznej, plików skompresowanych ZIP i GZIP. Wymagane jest, aby możliwe było włączenie lub wyłączenie usługi antywirus w poszczególnych strefach bezpieczeństwa, oraz możliwość włączenia lub wyłączenia reagowania na określone sygnatury.
      ii. Sonda IDP (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. Sygnatury powinny umożliwiać wykrywanie i blokowanie zdarzeń takich jak:

korzystanie z programów do wymiany plików P2P (np. Limewire, BitTorrent, eMule, etc.), korzystanie z komunikatorów internetowych (np. Yahoo Messenger, Gadu-Gadu, Skype, etc.), ataki typu backdoor, exploit, SQL-Injection, etc. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych.

iii. Sieciowa ochrona antyspyware, zapewniająca skanowanie ruchu HTTP, FTP, SMTP, POP3, IMAP. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych.

iv. Usługa filtrowania treści stron WWW, zapewniająca blokowanie apletów Java, aplikacji Active-X, plików cookie, definiowanie białych i czarnych list stron www, definiowanie słów kluczowych umożliwiających zablokowanie strony w przypadku ich wystąpienia. Dodatkowo wymagane jest tworzenie reguł filtrowania treści dla poszczególnych grup użytkowników umożliwiających filtrowanie treści w oparciu o informacje z zewnętrznych serwerów zawierających bazę stron zestawionych w co najmniej 56 kategoriach. Wymagane jest, aby mechanizm filtrowania treści uwzględniał także filtrowanie stron HTTPS oraz możliwość włączenia lub wyłączenia mechanizmu filtrowania treści w poszczególnych strefach bezpieczeństwa i zdefiniowanie domyślnej reguły dla każdej ze stref działającej niezależnie od uprawnień poszczególnych użytkowników.

v. Usługa Firewall aplikacji umożliwiająca definiowanie własnych sygnatur oraz reakcji urządzenia w przypadku wykrycia ruchu zgodnego z wprowadzonymi sygnaturami.

vi. Ochrona poczty elektronicznej w oparciu o białe/czarne listy nadawców oraz serwery RBL.

f. Wymagana jest taka możliwość skonfigurowania połączeń IPSec VPN client-site, aby cały ruch z połączonych do urządzeń klientów przesyłany był poprzez urządzenia i możliwe było jego skanowanie przez mechanizmy antywirus, antyspyware, IDP, filtrowania treści.

g. Wymaga się, aby na urządzeniach możliwe było włączenie blokowania ruchu przesyłanego pomiędzy strefami w przypadku, kiedy na stacjach roboczych lub serwerach nie będzie zainstalowanego odpowiedniego oprogramowania antywirusowego, lub oprogramowanie to będzie miało nieaktualne sygnatury.

h. Wymaga się, aby mechanizmy antywirus, antyspyware i sonda IDP nie posiadały ograniczeń co do wielkości skanowanych plików

9. Monitorowanie i raportowanie zdarzeń

a. Wymagane jest dostarczenie dedykowanego oprogramowania (instalowanego na zewnętrznym serwerze) zapewniającego monitorowanie, rejestrację i graficzną (w postaci tabel i wykresów) prezentację danych przesłanych z urządzenia firewall dotyczących ruchu, oraz zagrożeń sieciowych. Niezbędne dane to średnia zajętość łącza w podziale na dni i godziny, wykorzystanie pasma przez każdego z

użytkowników, informacje dotyczące przeglądanych witryn przez każdego z użytkowników sieci informatycznej, informacje dotyczące użytkowników łamiących zasady przeglądania witryn, informacje dot. ataków, detekcji intruzów, zagrożeń antywirusowych. Dane muszą mieć możliwość wydruku.

10. Wsparcie techniczne i gwarancja
    a. Wymagane jest aby dostarczane urządzenia objęte były okresem gwarancji przez okres 3 lat, z możliwością przedłużenia na dłuższy okres czasu. Wymagane jest, aby w ramach gwarancji uszkodzone urządzenie zostało wymienione w ciągu 24 godzin od chwili zgłoszenia niesprawności.
    b. Wymagane jest, aby urządzenia objęte było wsparciem technicznym 24x7, realizowanym przez producenta przez okres 3 lat z możliwością przedłużenia na dłuższy okres czasu

11. Wykonawca musi przedłożyć informację o proponowanych produktach w formie tabeli zawierającej w/w wymagania techniczne. (załącznik nr 6 do SIWZ).

IV. UWAGA DOTYCZĄCA WSZYSTKICH GRUP:

Podane w rozdziale XV nazwy własne są przykładowe. Zamawiający dopuszcza możliwość składania ofert równoważnych. Jeżeli wykonawca składa ofertę równoważną musi przedłożyć informację o proponowanym produkcie zawierającą co najmniej nazwę i parametry techniczne.

Członkowie komisji przetargowej:

1. Agnieszka Kosmala
2. Janusz Żyliński
3. Rafał Zygmunt
4. Marek Boka
5. Mirella Wołłejszo

.....
Dyrektor Biura ds. Zamówień Publicznych

.....
Dyrektor Komórki merytorycznej