SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

SPRZĘT KOMPUTEROWY, ZABEZPIECZAJĄCY ORAZ OPROGRAMOWANIE

ZAMAWIAJĄCY:
RZĄDOWE CENTRUM BEZPIECZEŃSTWA
Ul. Stefana Batorego 5
02 – 591 Warszawa
Tel. 0 - 22 60 - 158 – 30
Fax 0 - 22 60 - 158 – 21

TRYB POSTĘPOWANIA
Przetarg nieograniczony

Nr sprawy 1/2P/RCB/2009

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

I Nazwa i adres Zamawiającego, sposób porozumiewania się z Wykonawcami oraz osoby wskazane do kontaktów

1. **RZĄDOWE CENTRUM BEZPIECZEŃSTWA** z siedzibą w Warszawie, przy ul. Stefana Batorego 5, kod pocztowy 02-591,NIP **521-349-25-50**, Regon **141500466** adres strony internetowej Zamawiającego: http://zamowienia.mswia.gov.pl.
2. Postępowanie prowadzi się z zachowaniem formy pisemnej, przy czym Zamawiający dopuszcza, aby wszelkie oświadczenia, wnioski, zawiadomienia i informacje przekazywane były faksem na numer: 0 - 22 60 - 158 – 30.
   Każda ze stron postępowania na żądanie drugiej niezwłocznie potwierdza fakt otrzymania przekazanego faksem oświadczenia, wniosku, zawiadomienia, bądź informacji.
3. Osobami uprawnionymi do kontaktu z Wykonawcami są:
   1) Pan Adam Wiewiorowski – 0 – 22 60 – 158 – 30;
   2) Pan Grzegorz Rysz – 0 – 22 60-158-21.

II Tryb udzielenia zamówienia

Postępowanie prowadzone jest w oparciu o przepisy ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2007r. Nr 223 poz. 1655 ze zm.) zwanej dalej „pzp", w trybie przetargu nieograniczonego o wartości mniejszej niż kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 pzp.

III Opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup wraz z dostawą do siedziby Zamawiającego sprzętu komputerowego, zabezpieczającego oraz oprogramowania w podziale na 3 zadania.
Zgodnie z art. 36 ust. 2 pkt 1) ustawy pzp Zamawiający dopuszcza składanie ofert częściowych w zakresie opisanym poniżej dla poszczególnych zadań:

III A. ZADANIE I:

1. **sprzęt komputerowy:**
   a. SERWER 1;
   b. SERWER 2;
2. **Microsoft Windows Server 2008 Standard, w tym:**
   a. serwerowe – 3 licencje;
   b. dla użytkowników - 50 licencji;
3. **Microsoft Exchange Serwer 2007 Standard , w tym:**
   a. serwerowe – 1 licencja;
   b. dla użytkowników – 50 licencji;
4. **Microsoft Windows XP Pro SP 2PL – 1 licencja.**

III. B. ZADANIE II:

Sprzęt zabezpieczający:

a. urządzenie zabezpieczające sieć (typu firewall);
b. urządzenie zbierające i analizujące zdarzenia (analizer).

III. C. ZADANIE III:

Kompleksowy system ochrony poczty - 1 sztuka.

1. Szczegółowy zakres przedmiotu zamówienia został zawarty w następujących załącznikach:
   1) załącznik nr 6 – opis minimalnych parametrów technicznych - **ZADANIE I;**
   2) załącznik nr 7 – opis minimalnych parametrów technicznych - **ZADANIE II;**

3) załącznik nr 8 – opis minimalnych parametrów technicznych - **ZADANIE III;**

2. Ewentualne nazwy użyte przez Zamawiającego do opisu sprzętu stanowiącego przedmiot zamówienia należy traktować jako pomocnicze, wskazujące minimalne parametry techniczne.
3. Dostawca jest zobowiązany dostarczyć do sprzętu komplet okablowania umożliwiający prawidłowe uruchomienie sprzętu.
4. Gwarancja nie może ograniczać praw Zamawiającego do instalowania i wymiany w zakupionych serwerach modułów, standardowych kart i urządzeń (wyklucza się użycie jakichkolwiek plomb).
5. Zgodnie ze Wspólnym Słownikiem Zamówień (CPV) przedmiot zamówienia obejmuje zakres określony kodami: **48.82.00.00-2 – Serwery, 32.42.00.00-3 – Urządzenia sieciowe, oprogramowanie: 32.42.50.00 – 8 – Sieciowy system operacyjny, 48.22.30.00 – 7 – Pakiety oprogramowania do poczty elektronicznej, 48.62.00.00 – 0 – System operacyjny.**
6. Zamawiający nie przewiduje zamówień uzupełniających.
7. Na podstawie art. 36 ust. 5 pzp Zamawiający zastrzega, że cały zakres zamówienia Wykonawca zobowiązany jest wykonać siłami własnymi.
8. Zamawiający nie dopuszcza ofert wariantowych.
9. Zamawiający nie dopuszcza ofert równoważnych.
10. Wykonawca jest związany złożoną ofertą 30 dni od wyznaczonej w SIWZ daty składania ofert.

IV Termin wykonania zamówienia

Wymagany przez Zamawiającego termin realizacji zamówienia: **15 dni** od daty podpisania umowy.

V Opis warunków udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków – dla wszystkich ZADAŃ

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

1) nie podlegają wykluczeniu na podstawie art. 24 pzp,
2) spełniają warunki, o których mowa w art. 22 pzp.

Ocena spełniania ww. warunków dokonana zostanie, zgodnie z formułą „spełnia - nie spełnia", w oparciu o informacje zawarte w dokumentach i oświadczeniach złożonych przez Wykonawcę do postępowania. Z treści załączonych dokumentów musi wynikać jednoznacznie, iż w/w warunki Wykonawca spełnił.

VI Wykaz oświadczeń lub dokumentów, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu – dla wszystkich zadań:

Na potwierdzenie spełnienia warunków określonych w **części V SIWZ,** Zamawiający żąda przedstawienia:

1) aktualnego odpisu z właściwego rejestru albo aktualnego zaświadczenia o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej, wystawionego **nie wcześniej niż 6 miesięcy** przed upływem terminu składania ofert;
2) na potwierdzenie, iż Wykonawca nie podlega wykluczeniu, Zamawiający żąda przedstawienia oświadczenia o niewykluczeniu z art. 24 ust. 1 pkt 1 – 9 pzp - sporządzonego zgodnie z formularzem załącznika nr 2 do niniejszej SIWZ.
3) Na potwierdzenie spełnienia warunków udziału w postępowaniu Zamawiający żąda przedstawienia oświadczenia o spełnianiu wymogów, o których mowa w art. 22 ust. 1

pkt 1 – 3 pzp - sporządzonego zgodnie z formularzem załącznika nr 3 do niniejszej SIWZ.

Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zobowiązany jest, odpowiednio złożyć dokumenty określone w rozporządzeniu Prezesa Rady Ministrów z dnia 19 maja 2006 roku *w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy oraz form, w jakich te dokumenty mogą być składane* (Dz. U. z 2006r. Nr 87, poz. 605 ze zm.).

W odniesieniu do Wykonawców wspólnie ubiegających się o udzielenie zamówienia /konsorcjum/, każdy z Wykonawców wspólnie ubiegających o udzielenie zamówienia, musi we własnym imieniu złożyć dokumenty/oświadczenia wymienione w części VI. Pozostałe dokumenty/oświadczenia, jeżeli potwierdzają spełnianie warunków przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia - składane są w ich imieniu wspólnie.
Oferta uczestników konsorcjum musi zawierać wskazanie pełnomocnika do reprezentowania członków konsorcjum w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
Uwaga! treść pełnomocnictwa powinna dokładnie określać zakres umocowania.

VII Opis sposobu przygotowania oferty

1. Forma dokumentów składanych wraz z ofertą musi być zgodna z formą określoną w § 4 rozporządzenia Prezesa Rady Ministrów z dnia 19 maja 2006 roku *w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy oraz form, w jakich te dokumenty mogą być składane* (Dz. U. z 2006r. Nr 87, poz. 605 ze zm.).
2. Zamawiający zaleca wykorzystanie formularzy opracowanych przez Zamawiającego. Wykonawca może zastosować formularze wykazów, informacji i oświadczeń opracowane samodzielnie, z zastrzeżeniem - ich treść musi zawierać co najmniej treść zgodną z załącznikami opracowanymi przez Zamawiającego.
3. Oferta musi zawierać:
   1) dokumenty wymienione w części VI SIWZ,
   2) formularz oferty, sporządzony zgodnie z formularzem załącznika nr 1A dla ZADANIA I , załącznika nr 1B dla ZADANIA II lub załącznika nr 1C dla ZADANIA III,
   3) Oświadczenie Wykonawcy o zgodności parametrów technicznych proponowanego sprzętu z parametrami opisanymi przez Zamawiającego dla ZADANIA I, II i III.

   dla ZADANIA I:
   4) Deklaracja zgodności CE – dla obu serwerów.
   5) Certyfikaty lub inne dokumenty np. oświadczenie Wykonawcy, wydruk ze strony internetowej potwierdzające, że serwery znajdują się na liście Windows Server Catalog of Tested Products i posiadają status Certified for Windows dla systemów Windows Server 2008 x86 i Windows Server 2008 x64.
   6) Certyfikaty lub inne dokumenty np. oświadczenie Wykonawcy, wydruk ze strony internetowej potwierdzające, że serwery znajdują się na liście RedHat Certified Hardware i posiadać status Certified (Supported) dla systemów RHEL5-QU1/RHEL4-QU6 i/lub RHEL5-QU1.
   7) Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy lub firmy serwisującej, przejmie on na siebie wszelkie zobowiązania związane z serwisem.

   dla ZADANIA II:
   8) Deklaracja zgodności CE dla obu urządzeń;

9) Certyfikaty: UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus lub inne dokumenty np. oświadczenie Wykonawcy, że sprzęt spełnia ww. normy – dla urządzenia zabezpieczającego sieć.

dla ZADANIA III:

10) Deklaracja zgodności CE.

4. Urządzenia i podzespoły muszą mieć podane nazwy i marki producentów lub inne dane umożliwiające ich identyfikację.
5. Ofertę trzeba sporządzić na piśmie w języku polskim, pismem maszynowym lub ręcznie w sposób czytelny, z wykorzystaniem trwałych nośników pisma.
6. Zapisane strony oferty powinny być ponumerowane.
7. Wszelkie poprawki powinny być dokonane poprzez przekreślenie błędnego zapisu i wstawienie obok poprawnego oraz parafowane przez osobę podpisującą ofertę. Parafka (podpis) winna być naniesiona w sposób umożliwiający identyfikację podpisu (np. wraz z imienną pieczątką osoby).
8. Dokumenty powinny zostać połączone w sposób uniemożliwiający ich przypadkową dekompletację /bez udziału osób trzecich/ oraz uniemożliwiający zmianę jej zawartości bez widocznych śladów jej naruszenia tzn. zszyte, spięte lub przesznurowane, a końce sznurka trwale zabezpieczone.
9. W przypadku, gdy Wykonawca umieszcza w ofercie informacje stanowiące tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, musi umieścić informację o ich zastrzeżeniu. Zamawiający dopuszcza spięcie i umieszczenie dokumentów zastrzeżonych, w oddzielnej wewnętrznej kopercie z oznakowaniem *„tajemnica przedsiębiorstwa"*. Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności, tzn. zastrzegł składając ofertę, iż nie mogą być one udostępnione innym uczestnikom postępowania (art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji* /Dz. U. z 2003r. Nr 153, poz. 1503 z późn. zm./)
10. Oferta powinna zawierać spis dokumentów – sporządzony zgodnie z załącznikiem nr 4.
11. Ofertę należy umieścić w dwóch zamkniętych, nieprzejrzystych kopertach, zewnętrznej niezawierającej nazwy Wykonawcy, oznaczonej:

„Sprzęt komputerowy, zabezpieczający oraz oprogramowanie"
Rządowe Centrum Bezpieczeństwa
Warszawa, ul. Stefana Batorego 5
Nie otwierać – dostarczyć do rąk Przewodniczącego Komisji Przetargowej

oraz wewnętrznej, oznaczonej nazwą i adresem Wykonawcy.

12. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

VIII Miejsce, termin składania i otwarcia ofert

1. Oferty należy składać w kancelarii ogólnej Rządowego Centrum Bezpieczeństwa, Warszawa, ul. Stefana Batorego 5 pokój nr 211 do dnia **28.01.2008 r.** do godz. 10.00. – wejście przez biuro przepustek MSWiA od strony ul. Rakowieckiej.
2. Otwarcie ofert nastąpi w Rządowym Centrum Bezpieczeństwa, Warszawa, ul. Stefana Batorego 5 pokój nr 203 w dniu **28.01.2008**. o godz. 10.30.

UWAGA!!!
Wykonawcy składający ofertę osobiście lub zainteresowani udziałem w otwarciu ofert proszeni są o uwzględnienie czasu niezbędnego na przeprowadzenie procedur związanych z wejściem do siedziby Zamawiającego – ok. 20 min.

IX Opis sposobu obliczenia ceny

1. Cenę oferty należy obliczyć uwzględniając zakres zamówienia określony w zadaniu.
2. Ceny jednostkowe proszę podawać z dokładnością do 0,01 zł.
3. Podstawą obliczenia ceny oferty są materiały przekazane przez Zamawiającego: SIWZ wraz z załącznikami.
4. Cena oferty musi uwzględniać wszystkie elementy oraz wykonanie wszystkich prac i czynności związanych z realizacją przedmiotu zamówienia.

X Opis kryteriów oceny ofert, ich znaczenie i sposób oceny ofert dla obu ZADAŃ

Kryterium oceny ofert, które Zamawiający zastosuje celem wyłonienia najkorzystniejszej oferty przedstawia się w sposób następujący:

cena -znaczenie 100 %

Sposób obliczenia punktacji:

najniższa cena ze wszystkich ocenianych ofert x 100
---------- = ilość uzyskanych punktów
cena z oferty ocenianej

XI Informacje o formalnościach, po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego – dla obu ZADAŃ

1. Umowa zostanie zawarta w treści przedstawionej Wykonawcom w formie załącznika nr 5 do niniejszej SIWZ.
2. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, nie później niż w dniu podpisania umowy należy dostarczyć do siedziby Zamawiającego umowę regulującą współpracę tych Wykonawców. Umowa musi zawierać:
   a. określenie celu gospodarczego,
   b. oznaczenie czasu trwania umowy, obejmującego okres realizacji przedmiotu zamówienia, gwarancji lub/i rękojmi,
   c. wykluczenie możliwości wypowiedzenia umowy przez któregokolwiek z jej członków do czasu wykonania zamówienia oraz upływu czasu rękojmi lub/i gwarancji,
   d. zakaz zmian w umowie bez zgody Zamawiającego.

XII Środki ochrony prawnej przysługujące wykonawcy w toku postępowania

W niniejszym postępowaniu przysługują Wykonawcom środki ochrony prawnej opisane w dziale VI pzp.

DYREKTOR
RZĄDOWEGO CENTRUM BEZPIECZEŃSTWA
z up. Damian JAKUBOWSKI

Warszawa, 19 stycznia 2009r.

WYKAZ ZAŁĄCZNIKÓW I FORMULARZY:

1) załącznik nr 1A - formularz „OFERTA – ZADANIE I";
2) załącznik nr 1B - formularz „OFERTA – ZADANIE II";
3) załącznik nr 1C - formularz „OFERTA – ZADANIE III";
4) załącznik nr 2 - formularz oświadczenia - zgodnie z art. 24 ust. 1 pkt 1 – 9 ustawy pzp;
5) załącznik nr 3 - formularz oświadczenia - zgodnie z art. 22 ust. 1 pkt 1 – 3 ustawy pzp;
6) załącznik nr 4 – formularz „SPIS DOKUMENTÓW";
7) załącznik nr 5 – „UMOWA";
8) załącznik nr 6 – opis minimalnych parametrów technicznych - ZADANIE I;
9) załącznik nr 7 – opis minimalnych parametrów technicznych - ZADANIE II;
10) załącznik nr 8 – opis minimalnych parametrów technicznych - ZADANIE III.

Załącznik nr 1A

.....
pieczęć Wykonawcy

Warszawa, dnia ___.___.2009r.

NAZWA POSTĘPOWANIA:
„Sprzęt komputerowy, zabezpieczający i oprogramowanie – ZADANIE I"

O F E R T A

Dane Wykonawcy:

Pełna nazwa Wykonawcy:	
.....	
Adres Wykonawcy:	
Nr REGON	Nr tel. .....
Nr NIP	Nr fax .....
e – mail	

1. Oferujemy wykonanie przedmiotu zamówienia w pełnym zakresie rzeczowym i na warunkach określonych w Specyfikacji Istotnych Warunków Zamówienia za cenę:

Przedmiot	**Cena / brutto/ za wykonanie przedmiotu zamówienia**
Wykonanie całego przedmiotu zamówienia określonego w SIWZ	.....pln
słownie:	
.....	

2. Dostawa będąca przedmiotem zamówienia zostanie wykonana w terminie nie dłuższym niż 15 dni od daty podpisania umowy.
3. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia (w tym ze wzorem umowy) oraz przyjmujemy warunki w niej zawarte.
4. Oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w SIWZ tj. 30 dni od daty otwarcia ofert.
5. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
6. Oświadczamy, że serwis gwarancyjny będzie prowadzony zgodnie z warunkami zawartymi w załączniku nr 6 do Specyfikacji Istotnych Warunków Zamówienia p.n. „Opis przedmiotu zamówienia –Zadanie I".

.....
pieczęć i podpis osoby uprawnionej

.....
pieczęć Wykonawcy

O F E R T A - Zestawienie cenotwórcze

L.p.	rodzaj sprzętu	ilość	wartość za sztukę /netto/	cena za sztukę /brutto/	wartość za całość zamówienia /netto/	cena za całość zamówienia /brutto/
I.	**S E R W E R Y**					
1.	**Serwer nr 1**	1 sztuka	_____,__	_____,_____	_____,_____	_____,_____
2.	**Serwer nr 2**	1 sztuka	_____,__	_____,_____	_____,_____	_____,_____
II.	**O P R O G R A M O W A N I E**					
1.	**Microsoft Windows Serwer 2008 Standard**					
a.	**serwerowe**	3 licencje	_____,__	_____,_____	_____,_____	_____,_____
b.	**dla użytkowników**	50 licencji	_____,__	_____,_____	_____,_____	_____,_____
c.	**nośnik**	1 sztuka	_____,__	_____,_____	_____,_____	_____,_____

2.	**Microsoft Exchange Serwer 2007 Standard**					
a.	**serwerowe**	1 licencja	_____,__	_____,_____	_____,_____	_____,_____
b.	**dla użytkowników**	50 licencji	_____,__	_____,_____	_____,_____	_____,_____
c.	**nośnik**	1 sztuka	_____,__	_____,_____	_____,_____	_____,_____
3.	**Microsoft Windows XP Pro SP 2PL**	1 licencja	_____,__	_____,_____	_____,_____	_____,_____
a.	**nośnik**	1 sztuka	_____,__	_____,_____	_____,_____	_____,_____
III.	**RAZEM CAŁOŚĆ ZAMOWIENIA**				_____,_____	_____,_____

1.	słownie netto za całość zamówienia:	.....
2.	słownie brutto za całość zamówienia:	.....

.....
pieczęć Wykonawcy

O F E R T A – ARKUSZ ZGODNOŚCI

Serwer nr 1		
Parametr	**Wymagania minimalne**	**Oferowane parametry**
Obudowa	Maksymalnie 2U do instalacji w standardowej szafie RACK 19", dostarczona wraz z szynami	
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów, szyna FSB do 1333 MHz. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	
Procesor	Quad Core Intel Xeon E5440, 2X6MB Cache,2.8GHz, 1333MHz FSB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.	

RAM	4 GB DDR2 SDRAM 667MHz FBD, możliwa rozbudowa do 64GB	
Zabezpieczenia pamięci RAM	ECC, SDDC (lub równoważny), Online Spare Row, memory mirror	
Gniazda PCI	Minimum 3 x PCI-Express z czego minimum 2 x PCI-E x8	
Interfejsy sieciowe	Zintegrowana 2 x 10/100/1000 z możliwością obsługi stosu TCP/IP – TOE	
Napęd optyczny	Wewnętrzny napęd DVD-ROM	
Dyski twarde	2 x 450GB typu HotPlug SAS 3,5“ 15krpm, skonfigurowane jako RAID 1, możliwość rozbudowy o cztery dodatkowe dyski twarde	
Kontroler RAID	Zintegrowany. Pamięć podręczna minimum 256MB, z podtrzymaniem bateryjnym, możliwe konfiguracje 0, 1, 10, 5, 50, 6, 60	
Porty	5 x USB 2.0 z czego 2 na przednim panelu obudowy, 2 na tylnym panelu obudowy i jeden wewnętrzny, 2 x RJ-45, VGA	
Video	Zintegrowana karta graficzna	

Elementy redundantne HotPlug	Wentylatory, zasilacze	
Zasilacze	Redundantne, Hot-Plug o mocy maksymalnie 750W każdy	
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM 1.2	
Certyfikaty	Deklaracja zgodności CE. Oferowany model serwera musi znajdować się na liście Windows Server Catalog of Tested Products i posiadać status Certified for Windows dla systemów Windows Server 2008 x86 i Windows Server 2008 x64. Oferowany model serwera musi znajdować się na liście RedHat Certified Hardware i posiadać status Certified (Supported) dla systemów RHEL5-QU1/RHEL4-QU6 i/lub RHEL5-QU1.	
Warunki gwarancji dla serwera	• 3 lata na miejscu u klienta. • Możliwość zgłaszania usterek w trybie 24/7/365. • Czas reakcji serwisu w ciągu następnego dnia roboczego. • Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy lub firmy serwisującej, przejmie on na	

	siebie wszelkie zobowiązania związane z serwisem. • W przypadku awarii dysku twardego uszkodzony nośnik pozostaje u Zamawiającego.	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim i angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	

.....

pieczęć Wykonawcy

Serwer nr 2		
Parametr	**Wymagania minimalne**	**Oferowane parametry**
Obudowa	Maksymalnie 1U do instalacji w standardowej szafie RACK 19”	
Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora, również w technologii quad-core, szyna FSB minimum 1066 MHz lub szybsza. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Procesor	Quad Core Intel Xeon X3360, 2.83GHz, 2x6MB Cache, 1333MHz FSB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.	

RAM	GB DDR2 Dual Rank, możliwa rozbudowa do 8GB	
Zabezpieczenia pamięci RAM	ECC	
Gniazda PCI	2 x PCI Express w tym jedno x8	
Interfejsy sieciowe	2 x 10/100/1000	
Napęd optyczny	Wewnętrzny napęd DVD-ROM	
Dyski twarde	2x minimum 250GB SATA, skonfigurowane w RAID1	
Video	Zintegrowana karta graficzna	
Porty I/O	Wbudowany porty: 2xPS/2, szeregowy, minimum 4 x USB 2.0 wyprowadzone z czego 2 na przednim panelu i dwa z tyłu	
Zasilacz	Zasilacz o mocy max. 345W	
Szyny montażowe	Statyczne, umożliwiające instalację w szafie 19'', standard Versa	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim i angielskim Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela	

Certyfikaty	Deklaracja zgodności CE. Oferowany model serwera musi znajdować się na liście Windows Server Catalog of Tested Products i posiadać status Designed for Windows dla systemów Windows Server 2003 x86 i Windows Server 2003 x64 oraz Certified for Windows dla systemów Windows Server 2008 x86 i Windows Server 2008 x64. Oferowany model serwera musi znajdować się na liście RedHat Certified Hardware i posiadać status Certified (Supported) dla systemu RHEL5-QU1/RHEL4-QU6 i/lub RHEL5-QU1.	
Warunki gwarancji dla serwera	• 3 lata na miejscu u klienta. • Możliwość zgłaszania usterek w trybie 24/7/365. • Czas reakcji serwisu do końca następnego dnia roboczego. • Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy lub firmy serwisującej, przejmie on na siebie wszelkie zobowiązania związane z serwisem. • W przypadku awarii dysku twardego uszkodzony nośnik pozostaje u Zamawiającego.	

.....

pieczęć Wykonawcy

Oprogramowanie	
Wymagania minimalne	**Oferta**
Microsoft Windows Server 2008 Standard (z możliwością zamiennej instalacji Microsoft Windows Serwer 2003 Standard)	
Microsoft Exchange Server 2007 Standard	
Windows XP Pro z Sp2	
Sposób licencjonowania: oprogramowanie ma być licencjonowane w ramach Umowy Licencyjnej Microsoft Open (typu Goverment). Ponadto zaproponowane oprogramowanie musi posiadać taki sposób licencjonowania, który zapewni jego instalację na komputerze (komputerach) inne niż te, na których pierwotnie zainstalowano oprogramowanie, pod warunkiem wcześniejszej deinstalacji z tego komputera (komputerów).	

.....

pieczęć Wykonawcy

Załącznik nr 1B

.....
pieczęć Wykonawcy

Warszawa, dnia ___.___.2009r.

NAZWA POSTĘPOWANIA:
„Sprzęt komputerowy, zabezpieczający i oprogramowanie – ZADANIE II"

O F E R T A

Dane Wykonawcy:

Pełna nazwa Wykonawcy:	
Adres Wykonawcy:	
Nr REGON	Nr tel. .....
Nr NIP	Nr fax .....
e – mail	

1. Oferujemy wykonanie przedmiotu zamówienia w pełnym zakresie rzeczowym i na warunkach określonych w Specyfikacji Istotnych Warunków Zamówienia za cenę:

Przedmiot	**Cena / brutto/ za wykonanie przedmiotu zamówienia**
Wykonanie całego przedmiotu zamówienia określonego w SIWZ	.....pln
słownie:	

2. Dostawa będąca przedmiotem zamówienia zostanie wykonana w terminie nie dłuższym niż 15 dni od daty podpisania umowy.
3. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia (w tym ze wzorem umowy) oraz przyjmujemy warunki w niej zawarte.
4. Oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w SIWZ tj. 30 dni od daty otwarcia ofert.
5. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
6. Oświadczamy, że serwis gwarancyjny będzie prowadzony zgodnie z warunkami zawartymi w załączniku nr 7 do Specyfikacji Istotnych Warunków Zamówienia p.n. „Opis przedmiotu zamówienia – Zadanie II".

.....
pieczęć i podpis osoby uprawnionej

.....
pieczęć Wykonawcy

O F E R T A - Zestawienie cenotwórcze

L.p.	rodzaj sprzętu	ilość	wartość za sztukę /netto/	cena za sztukę /brutto/	wartość za całość zamówienia /netto/	cena za całość zamówienia /brutto/
I.	**S P R Z Ę T Z A B E Z P I E C Z A J Ą C Y**					
1.	**Urządzenie zabezpieczające sieć (typu firewall)**	1 sztuka	_____,__	_____,____	_____,_____	_____,_____
2.	**Urządzenie zbierające i analizujące zdarzenia (analizer)**	1 sztuka	_____,__	_____,__	_____,_____	_____,_____
II.	**RAZEM CAŁOŚĆ ZAMOWIENIA**				_____,_____	_____,_____
1.	słownie netto za całość zamówienia:	....				
2.	słownie brutto za całość zamówienia:	....				

.....
pieczęć Wykonawcy

O F E R T A – ARKUSZ ZGODNOŚCI

I. Urządzenie zabezpieczające sieć			
Lp.	**Parametr**	**Wymagania techniczne**	
1.	Architektura systemu ochrony	Główne urządzenie ochronne [gateway] nie może posiadać twardego dysku, w zamian ma używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu układu ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy, wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny, pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). Uwaga: Dziennik zdarzeń lub inne działania wymagające systemów dyskowych muszą być realizowane na dedykowanych do tego celu urządzeniach.	
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.	
3.	Ilość/rodzaj portów	Nie mniej niż **10** portów Ethernet 10/100/1000 Base-TX, oraz możliwość instalacji portów dodatkowego modułu **4** portów 1000 SFP.	

		Nie mniej niż **255** interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q	
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę ogniową klasy Stateful Inspection • ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM) • poufność danych - IPSec VPN oraz SSL VPN • ochronę przed atakami - Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających: • kontrolę treści – Web Filter [WF] • kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) • kontrolę pasma oraz ruchu [QoS i Traffic shaping] • kontrolę komunikatorów sieciowych (IM) oraz aplikacji P2P	
5.	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: jako router/NAT (3.warstwa ISO-OSI) lub jako most /transparent bridge . Możliwosc wdrożenia urządzenia bez istotnych modyfikacji topologii sieci.	
6.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma	

		gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).	
7.	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. • Nie mniej niż 3900 sygnatur ataków. • Aktualizacja bazy sygnatur ma się odbywać w sposób automatyczny poprzez sieć lub w sytuacjach awaryjnych ręcznie przy użyciu nośnika. • Możliwość wykrywania anomalii protokołów i ruchu	
8.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT.	
9.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.	
10.	Połączenia VPN	Wymagane nie mniej niż: • Tworzenie połączeń w topologii Site-to-site oraz Client-to-site • Dostawca musi udostępniać klienta VPN własnej	

		produkcji realizującego następujące mechanizmy ochrony końcówki: o firewall o antywirus o web filtering o antyspam • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	
11.	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory bez dodatkowych opłat licencyjnych.	
12.	Wydajność	Obsługa nie mniej niż **500 000** jednoczesnych połączeń i **20 000** nowych połączeń na sekundę Przepływność nie mniejsza niż **8 Gb/s** dla ruchu nieszyfrowanego i **6 Gb/s** dla VPN (3DES). Obsługa nie mniej niż **3 000** jednoczesnych tuneli VPN	

13.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive	
14.	Obudowa	Obudowa ma mieć możliwość zamontowania w szafie 19".	
15.	Zasilanie	Zasilanie z sieci 230V/50Hz.	
16.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: • haseł statycznych • haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla systemu urządzenie powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.	
17.	Certyfikaty	UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus.	

18.	Gwarancja i wsparcie	Wsparcie techniczne do zakupionych rozwiązań świadczone w trybie 24/7 (przez 7 dni w tygodniu, 24 godziny na dobę). Wsparcie realizowane przez inżynierów certyfikowanych przez producenta oferowanych rozwiązań. Czas reakcji na zgłoszone problemy nie przekraczający 4 godzin. Wsparcie techniczne obejmujące: pomoc w konfiguracji wspieranych rozwiązań, usuwanie skutków awarii systemu, analiza logów i alertów, pośrednictwo w kontaktach z producentem oferowanego rozwiązania,okresowe wizyty „prewencyjne" realizowane w czasie dogodnym dla Klienta, dostęp do lokalnego portalu wsparcia, oferującego informacje na temat nowych wersji oprogramowania, poprawek, FAQ etc.Przeprowadzenie szkolenia technicznego dla administratorów systemu. Gwarancja na okres min. 12 miesięcy	

.....

pieczęć Wykonawcy

II. Urządzenie zbierające i analizujące zdarzenia			
Lp.	**Parametr**	**Wymagania techniczne**	
1.	Architektura systemu	System logowania i raportowania powinien stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i hardware pochodziły od jednego producenta. Urządzenie powinno obsługiwać co najmniej dziesięć urządzeń sieciowych i współpracować z urządzeniem wyszczególnionym w pkt. I.	
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.	
3.	Parametry fizyczne systemu	Nie mniej niż 4 porty Ethernet 10/100 Base-TX Powierzchnia dyskowa - minimum 250 GB	

4.	Funkcjonalności podstawowe i uzupełniające	System musi zapewniać: 1. Składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników 2. Możliwość gromadzenia zawartości przesyłanych za pośrednictwem protokołów Web, FTP, email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci 3. Kwarantannę dla współpracujących z nim urządzeń. Kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki. 4. Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących 5. Wyświetlanie nowych logów w czasie rzeczywistym 6. Analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy 7. Analizę podatności stacji w sieci wraz z możliwością raportowania wykrytych luk 8. Export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych)	
5.	Aktualizacje sygnatur sprawdzeń	System musi zapewniać: 1. Planowanie aktualizacji bazy sprawdzeń w czasie (Scheduler)	

6.	Zarządzanie	System udostępnia: 1. Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH i konsolę szeregową	
7.	Zasilanie	Zasilanie z sieci 230V/50Hz.	
8.		Wsparcie techniczne do zakupionych rozwiązań świadczone w trybie 24/7 (przez 7 dni w tygodniu, 24 godziny na dobę). Wsparcie realizowane przez inżynierów certyfikowanych przez producenta oferowanych rozwiązań Czas reakcji na zgłoszone problemy nie przekraczający 4 godzin. Wsparcie techniczne obejmujące: pomoc w konfiguracji wspieranych rozwiązań, usuwanie skutków awarii systemu, analiza logów i alertów, pośrednictwo w kontaktach z producentem oferowanego rozwiązania,okresowe wizyty „prewencyjne" realizowane w czasie dogodnym dla Klienta, dostęp do lokalnego portalu wsparcia, oferującego informacje na temat nowych wersji oprogramowania, poprawek, FAQ etc. Przeprowadzenie szkolenia technicznego dla administratorów systemu. Gwarancja na okres min. 12 miesięcy	

.....

pieczęć Wykonawcy

Załącznik nr 1C

.....
pieczęć Wykonawcy

Warszawa, dnia ___.___.2009r.

NAZWA POSTĘPOWANIA:
„Sprzęt komputerowy, zabezpieczający i oprogramowanie – ZADANIE III"

O F E R T A

Dane Wykonawcy:

Pełna nazwa Wykonawcy:	
.....	
Adres Wykonawcy:	
Nr REGON	Nr tel. .....
Nr NIP	Nr fax .....
e – mail	

1. Oferujemy wykonanie przedmiotu zamówienia w pełnym zakresie rzeczowym i na warunkach określonych w Specyfikacji Istotnych Warunków Zamówienia za cenę:

Przedmiot	**Cena / brutto/ za wykonanie przedmiotu zamówienia**
Wykonanie całego przedmiotu zamówienia określonego w SIWZ	.....pln
słownie:	
.....	

2. Dostawa będąca przedmiotem zamówienia zostanie wykonana w terminie nie dłuższym niż 15 dni od daty podpisania umowy.
3. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia (w tym ze wzorem umowy) oraz przyjmujemy warunki w niej zawarte.
4. Oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w SIWZ tj. 30 dni od daty otwarcia ofert.
5. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
6. Oświadczamy, że serwis gwarancyjny będzie prowadzony zgodnie z warunkami zawartymi w załączniku nr 8 do Specyfikacji Istotnych warunków Zamówienia p.n. „Opis przedmiotu zamówienia – Zadanie III".

.....
pieczęć i podpis osoby uprawnionej

.....
pieczęć Wykonawcy

O F E R T A - Zestawienie cenotwórcze

L.p.	rodzaj sprzętu	ilość	wartość za sztukę /netto/	cena za sztukę /brutto/	wartość za całość zamówienia /netto/	cena za całość zamówienia /brutto/
1.	**Kompleksowy system ochrony poczty**	1 sztuka	_____,__	_____,____	_____,____	_____,____
2.	**RAZEM CAŁOŚĆ ZAMOWIENIA**				_____,____	_____,____
a.	słownie netto za całość zamówienia:	....				
b.	słownie brutto za całość zamówienia:	....				

.....
pieczęć Wykonawcy

O F E R T A – ARKUSZ ZGODNOŚCI

System kompleksowej ochrony poczty elektronicznej		
Lp.	**wymagania minimalne**	**oferta**
1	System musi zapewniać ochronę przed zagrożeniami związanymi z przesyłaniem poczty elektronicznej (wirusy, spam, phishing, niedozwolone treści, etc.), ochronę przeciwko atakom typu Odmowa dostępu do usług (Denial Of Service) oraz logować i zapobiegać enumeracji kont użytkowników chronionej domeny pocztowej (Directory Harvesting Attack).	
2	System musi zostać dostarczony w formie kompletnego, zamkniętego rozwiązania sprzętowego.	
3	Oferowane rozwiązanie musi być zgodne z obecnie użytkowanym systemem ochrony antywirusowej (instytucja korzysta z f-secura).	
4	Urządzenie musi zapewniać wydajność na poziomie minimum 40.000 wiadomości skanowanych w ciągu godziny.	

5	Obudowa musi umożliwić montaż w standardowej szafie RACK 19" i posiadać rozmiar 1U.	
6	Urządzenie musi posiadać minimum dwa interfejsy sieciowe w standardzie Gigabit BaseT.	
7	Pliki systemu operacyjnego, logi, kwarantanna, etc. muszą być przechowywane na dyskach pracujących w standardzie minimum RAID 1, użyte dyski twarde muszą być tak zainstalowane aby umożliwiać wymianę bez wstrzymywania pracy urządzenia.	
8	System w momencie dostarczenia lub po odtworzeniu musi zawierać: - zestaw predefiniowanych reguł i polityk dla wszystkich modułów filtrujących (AV, antyspam, kontrola treści), - powinien zawierać zestaw predefiniowanych raportów.	
9	Zarządzanie systemem powinno być możliwe przy użyciu bezpiecznego połączenia https przez przeglądarkę internetową, lub rozwiązanie równoważne.	

10	System musi: - pracować jako brama smtp i być niezależnym od rodzaju stosowanych, chronionych serwerów pocztowych, - zapewniać możliwość szyfrowania przesyłek za pomocą protokołu Transport Layer Security w warstwie sieciowej, - umożliwiać korzystanie z zewnętrznych serwerów RBL, - zapewniać wsparcie dla standardu z Sender Policy Framework, - 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, - zapewniać inteligentne rozpoznawanie typów analizowanych załączników, - posiadać lokalną kwarantannę dla zainfekowanych wiadomości, - zapewniać możliwość tworzenia kilku polityk ochrony antywirusowej przydzielanych w oparciu o: adresy IP serwera nadawcy, adres email nadawcy/odbiorcy wiadomości, - zapewniać automatyczną ocenę reputacji źródła przesyłanego mail'a (na podstawie ilości połączeń, procentowej ilości maili z wirusami, procentowej ilości wiadomości zakwalifikowanych jako spam), - posiadać moduł antyspamowy zapewniający analizę statystyczną wiadomości na podstawie minimum 200.000 atrybutów maila, - zapewniać użytkownikom końcowym możliwość zarządzania wiadomościami trafiającymi do ich personalnej kwarantanny, - zapewniać możliwość opcjonalnego uwierzytelniania użytkownika w celu zmian parametrów własnego folderu kwarantanny, - umożliwiać następujące operacje na wiadomościach przechowywanych w	

	obszarze kwarantanny: usunięcie wiadomości, przesłanie do odbiorcy, automatyczna zgłoszenie przypadków złej klasyfikacji wiadomości do producenta systemu, - 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, - zapewniać możliwość zdefiniowania wielu administratorów o zróżnicowanych uprawnieniach, - zapewniać automatyczną aktualizację sygnatur antywirusowych, silników skanujących, modułów systemu antyspamowego, oprogramowania i systemu operacyjnego z serwera producenta.	
11	Ochrona antywirusowa powinna być realizowana przy pomocy minimum trzech niezależnych silników skanujących.	
12	Możliwość definiowania: - różnych sposobów postępowania z zainfekowanymi wiadomościami w zależności od rodzaju wykrytego wirusa, - reguły antyspamowych na poziomie całego urządzenia, grup użytkowników oraz pojedynczych użytkowników, - list zaufanych i blokowanych nadawców przez użytkowników końcowych, - wyglądu kwarantanny końcowego użytkownika zarówno co do jej szaty graficznej (np. możliwość umieszczenia znaku firmowego) jak i treści komunikatów.	
13	Aktualizacje sygnatur modułu antywirusowego muszą być dostępny nie rzadziej niż raz na 24 godziny (raz na dobę).	
14	Możliwość określenia postępowania z zabezpieczonymi wiadomościami (załączniki chronione hasłem, podpisane wiadomości, etc.).	

15	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.	
16	Listy użytkowników definiowane lokalnie, możliwość importu użytkowników z serwerów: Active Directory, LDAP, MS Exchange, Lotus Domino oraz plików (tekstowe, csv).	
17	Możliwość określania poziomu dostępu i akcji możliwych do wykonania w obrębie kwarantanny dla różnych użytkowników/grup użytkowników.	
18	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.	
19	Rozbudowany system raportowania zapewniający dostęp do minimum 45 różnych rodzajów graficznych raportów.	
20	Możliwość okresowej publikacji wybranych raportów jako strony WWW, przy pomocy wysyłanych automatycznie wiadomości email oraz jako pliki xml.	
21	Logowanie na lokalnym dysku twardym lub zewnętrznym serwerze syslog zdarzeń podejmowanych przez filtry oraz zdarzeń dotyczących komunikacji smtp.	
22	Możliwość definiowania i przeglądania wielu katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych.	

23	Dla wszystkich stworzonych folderów kwarantanny system zapewni możliwość ustawienia maksymalnego czasu przechowywania wiadomości a po jego upływie automatycznie je usunie.	
24	System zapewni administratorowi wskazanie folderu/ów, z których wysyłany będzie skrót informacji o wiadomościach przeniesionych do personalnej kwarantanny użytkownika.	
25	Możliwość zapisu i odtworzenia konfiguracji.	
26	Wszystkie aktualizacje mają być pobierane z jednego miejsca a system komunikować się ze źródłem aktualizacji z częstotliwością narzuconą przez administratora systemu.	
27	System zapewni śledzenie historii wykonywania aktualizacji.	
28	Producent systemu powinien zapewnić możliwość zakupu aktualizacji systemu jednorazowo na okres roku, dwóch, trzech lat (lub dłużej).	
29	Urządzenie powinno być objęte gwarancją "NBD" – czas naprawy nie przekraczający jednego dnia roboczego.	
30	Gwarancja na okres min. 12 miesięcy, w przypadku awarii urządzenia dysk/dyski twarde pozostają u zamawiającego	
31	Deklaracja zgodności CE	

.....

pieczęć Wykonawcy

Załącznik nr 2

.....
/pieczęć Wykonawcy/

Warszawa, dnia ___.___.2009r.

NAZWA POSTĘPOWANIA:

„Sprzęt komputerowy, zabezpieczający i oprogramowanie"

ZADANIE I, ZADANIE I I, ZADANIE I I I

OŚWIADCZENIE

Oświadczam, iż

.....
/nazwa Wykonawcy/

nie podlega, na podstawie art. 24 ust. 1 pkt 1 – 9 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych /Dz. U. z 2007 r. Nr 223, poz. 1655/, wykluczeniu z postępowania o udzielenie zamówienia.

.....
/podpis i pieczęć osoby uprawnionej/

Załącznik nr 3

.....
/pieczęć Wykonawcy/

Warszawa, dnia ___.___.2009r.

NAZWA POSTĘPOWANIA:

„Sprzęt komputerowy, zabezpieczający i oprogramowanie"

ZADANIE I, ZADANIE I I, ZADANIE I I I

OŚWIADCZENIE

Oświadczam, iż zgodnie z art. 22 ust. 1 pkt 1 – 3 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych /Dz. U. z 2007 r. Nr 223, poz. 1655 ze zm. /

.....
/nazwa Wykonawcy/

1. posiada uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień;
2. posiada niezbędną wiedzę i doświadczenie oraz dysponuje potencjałem technicznym i osobami zdolnymi do wykonania zamówienia;
3. znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

.....
/podpis i pieczęć osoby uprawnionej/

Uwaga
Zgodnie z treścią art 22 ust. 1 pkt 2) Pzp Wykonawca może przedstawić w zakresie pkt. 2 niniejszego oświadczenia pisemne zobowiązanie innych podmiotów do udostępnienia potencjału technicznego i osób zdolnych do wykonywania zamówienia. Zobowiązanie należy dołączyć do oferty.

Załącznik nr 4

.....
/pieczęć Wykonawcy/

Warszawa, dnia ___.___.2009r.

NAZWA POSTĘPOWANIA:

„Sprzęt komputerowy, zabezpieczający i oprogramowanie"

ZADANIE I, ZADANIE I I, ZADANIE I I I

SPIS DOKUMENTÓW OFERTY

Lp.	Treść	Nr strony	Uwagi
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			

.....
/podpis i pieczęć osoby uprawnionej/

Załącznik nr 5

UMOWA

Zawarta w dniu ____.____.2008r. w Warszawie, pomiędzy Rządowym Centrum Bezpieczeństwa , z siedzibą w Warszawie, przy ul. Batorego 5, Nr NIP ___-___-__-__, Nr REGON _____, zwanym dalej w treści umowy „Zamawiającym", reprezentowanym przez:

1/. _____ _____ - _____;

a _____ z siedzibą _____ , Nr NIP ___-___-__-__, Nr REGON _____, prowadzącą działalność gospodarczą na podstawie _____ Nr _____, zwaną dalej w treści umowy „Wykonawcą", reprezentowaną przez:

1/. _____ _____ - _____;

§ 1

Zamawiający oświadcza, że niniejsza umowa zostaje zawarta z Wykonawcą, którego oferta została wybrana w wyniku postępowania przeprowadzonego w oparciu o przepisy ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych /Dz. U. z 2007r. Nr 223, poz. 1655 ze zm./ zwaną dalej „pzp", w trybie przetargu nieograniczonego o wartości mniejszej niż kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 pzp.

§ 2

1. Przedmiotem umowy jest dostawa sprzętu komputerowego _____ oraz oprogramowania.
2. Szczegółowe parametry techniczne, wraz z cenami jednostkowymi i specyfikacją ilościową zostały zawarte w ***załączniku*** do niniejszej umowy.

§ 3

1. Oprogramowanie specyficzne dla sprzętu (np. sterowniki), Wykonawca dostarczy na osobnym nośniku dla każdego urządzenia.
2. Oferowane oprogramowanie musi być dostarczone z dołączoną licencją i dokumentacją.
3. Dostarczone licencje (bezterminowe) będą wolne od roszczeń osób trzecich oraz bez możliwości ich wypowiedzenia.

§ 4

1. Wykonawca zobowiązuje się zrealizować zamówienie z zachowaniem należytej staranności, zasad bezpieczeństwa, dobrej jakości, właściwej organizacji pracy, zasad wiedzy technicznej, obowiązujących norm oraz przepisów prawa, na warunkach ustalonych niniejszą umową.
2. Dostarczone urządzenia są fabrycznie nowe, wolne od wad i zgodne z poziomem technologii istniejącym w dniu podpisania umowy.
3. Wykonawca zobowiązuje się wykonać cały zakres zamówienia siłami własnymi.

§ 5

1. Przedstawicielem Wykonawcy jest Pan/Pani _____ _____, który jest jednocześnie upoważniony ze strony Wykonawcy do podpisania protokołu przyjęcia – przekazania.
2. Przedstawicielem Zamawiającego jest Pan/Pani _____ _____, który jest jednocześnie upoważniony ze strony Zamawiającego do podpisania protokołu przyjęcia – przekazania.

§ 6

1. Wykonawca zobowiązuje się do realizacji przedmiotu umowy w nieprzekraczalnym terminie **15 dni od dnia podpisania umowy,** z uwzględnieniem czasu niezbędnego na dokonanie odbioru.
2. Fakt zgodności przedmiotu zamówienia z opisem przedmiotu umowy zostanie potwierdzony pod względem techniczno – jakościowym oraz ukompletowania *„Protokołem przyjęcia – przekazania"* podpisanym przez osoby odpowiedzialne za realizację umowy, wymienione w § 5, nie później niż w dniu następującym po dniu zgłoszenia przez Wykonawcę gotowości do odbioru, z zachowaniem procedur opisanych w § 7.

§ 7

1. Odbiór jakościowy i ilościowy odbędzie się w siedzibie Zamawiającego.
2. Wykonawca powiadomi Zamawiającego o gotowości do przeprowadzenia realizacji dostawy przesyłając informacje faxem na numer 0 -22 ___-___-___ nie później niż z 48-godzinnym wyprzedzeniem podając numer umowy, planowaną datę dostawy oraz numery seryjne sprzętu będącego przedmiotem zamówienia.
3. Odbiorowi jakościowemu podlegać będą wszystkie urządzenia stanowiące przedmiot dostawy.

4. Odbiór jakościowy będzie polegał na sprawdzeniu poprawności działania sprzętu wraz z oprogramowaniem.
5. W przypadku gdy sprzęt nie będzie działał poprawnie lub nie spełni wymagań konfiguracyjnych zostanie zwrócony Wykonawcy a procedura powtórzona.

§ 8

Nie później niż w dniu podpisania Protokołu przyjęcia – przekazania Wykonawca dostarczy Zamawiającemu:

1) nośniki dodatkowego oprogramowania np. sterowniki wraz z dokumentacją.
2) dokumentację techniczną oraz instrukcje urządzeń w języku polskim i angielskim.

§ 9

1. Na każdy egzemplarz przedmiotu umowy Wykonawca udziela gwarancji zgodnie ze złożoną ofertą na okres: **36** miesięcy, liczony od dnia podpisania protokołu przejęcia – przekazania.
2. Wykonawca odpowiada za wady fizyczne i prawne ujawnione w dostarczonym przedmiocie umowy i ponosi z tego tytułu wszelkie zobowiązania opisane w niniejszej umowie.
3. W szczególności jest odpowiedzialny względem Zamawiającego, jeżeli dostarczone wyroby:
   1) stanowią własność osoby trzeciej albo są obciążone prawem osób trzecich,
   2) mają wadę zmniejszającą ich wartość lub użyteczność wynikającą z ich przeznaczenia lub nie mają właściwości wymaganych przez Zamawiającego.
4. Wykonawca jest zobowiązany do usunięcia wad fizycznych w przedmiocie umowy lub do dostarczenia wyrobów wolnych od wad, jeżeli wady te ujawnią się w ciągu okresu gwarancji.
5. Utrata roszczeń z tytułu wad fizycznych nie następuje mimo upływu terminu gwarancji, jeżeli Wykonawca wadę podstępnie zataił.
6. Zamawiający może wykorzystać gwarancję producenta niezależnie od uprawnień wynikających z tytułu gwarancji określonej w niniejszej umowie.

§ 10

1. O wadzie fizycznej przedmiotu niniejszej umowy Zamawiający zawiadamia Wykonawcę bezpośrednio. Formę zawiadomienia stanowi telefoniczne zgłoszenie pod nr tel. ..... i potwierdzone w terminie 3 dni od daty ujawnienia wady, w formie pisemnej, faxem lub w formie elektronicznej.
2. W okresie gwarancji Wykonawca zapewni całodobowy kontakt w celu udzielania nieodpłatnych konsultacji i pomocy technicznej.

3. Zgłoszenia o awariach będą przyjmowane faksem i/lub w formie elektronicznej przez 24 godz./dobę. Nr telefonu - - -, adres email: _____.
4. W przypadku stwierdzenia w okresie gwarancji wad fizycznych w dostarczonych urządzeniach Wykonawca:
   1) rozpatrzy „Protokół reklamacji" w ciągu 2 dni roboczych od dnia jego otrzymania,
   2) usprawni wadliwe urządzenia w terminie 14 dni licząc od daty otrzymania zawiadomienia o wadzie fizycznej a w wypadku, gdy nie dokona ich usprawnienia, wymieni na nowe.
   3) usunie wady w dostarczonych urządzeniach w miejscu, w którym zostały one ujawnione lub na własny koszt dostarczy je do swojej siedziby, w celu ich usprawnienia,
   4) urządzenia wolne od wad dostarczy na własny koszt do miejsca, w którym wady zostały ujawnione zachowując termin określony w pkt 2),
   5) ponosi odpowiedzialność z tytułu przypadkowej utraty lub uszkodzenia urządzeń w czasie od przyjęcia ich do naprawy do czasu przekazania sprawnych urządzeń Zamawiającemu,
   6) przedłuży termin gwarancji o czas, w ciągu którego wskutek wady urządzeń objętych gwarancją uprawniony z gwarancji nie mógł z nich korzystać,
   7) dokona stosownych zapisów w karcie gwarancyjnej dotyczących zakresu wykonanych napraw oraz zmiany okresu udzielonej gwarancji,
   8) zwróci Zamawiającemu równowartość wadliwych urządzeń powiększoną o karę umowną w wysokości 10% ich ceny ofertowej brutto jeżeli nie wykona zobowiązań wynikających z pkt. 7).
5. Jeżeli w wykonaniu swoich obowiązków Wykonawca dostarczył Zamawiającemu zamiast wyrobu wadliwego taki sam lub nie gorszy wyrób nowy – wolny od wad – termin gwarancji biegnie na nowo od chwili jego dostarczenia.

§ 11

1. Gwarancja nie może ograniczać praw Zamawiającego do instalowania i wymiany w zakupionych serwerach modułów, standardowych kart i urządzeń (wyklucza się użycie jakichkolwiek plomb) –(zapis dotyczy umowy na zakup serwerów).
2. Uszkodzone dyski pozostają u Zamawiającego.
3. W przypadku zabrania sprzętu do serwisu, dyski pozostają u Zamawiającego, a ponadto Wykonawca jest zobowiązany dostarczyć sprzęt o takich samych lub lepszych parametrach, umożliwiających bezproblemowe uruchomienie dysków na sprzęcie zastępczym.

4. Do każdego sprzętu i urządzenia dostarczona będzie instrukcja w języku polskim i angielskim.

§ 12

1. Wynagrodzenie Wykonawcy zawiera wszelkie koszty związane z realizacją niniejszej umowy i wynosi _____,___ pln netto + _____,_____ pln VAT = ____,_____ pln brutto /słownie: _____ pln brutto/.
2. Ceny jednostkowe urządzeń zawiera załącznik do niniejszej umowy.
3. Wynagrodzenie zawiera wszystkie koszty realizacji zamówienia.

§ 13

1. Rozliczenie finansowe za realizację przedmiotu umowy odbędzie się na podstawie faktury wystawionej przez Wykonawcę po realizacji przedmiotu zamówienia i protokolarnym odbiorze.
2. Podstawę wystawienia faktury stanowi protokół przejęcia - przekazania podpisany przez upoważnionych przedstawicieli stron.
3. Protokół, o którym mowa w ust. 1, powinien zawierać co najmniej:
   1) datę sporządzenia protokołu,
   2) w ramach odbioru ilościowego - dokładne określenie przedmiotu odbioru,
   3) w ramach odbioru jakościowego - ewentualne uwagi i zastrzeżenia stron,
   4) potwierdzenie przejęcia – przekazania dokumentów, o których mowa w § 8,
   5) podpisy upoważnionych przedstawicieli stron.
4. Faktura będzie uregulowana przez Zamawiającego w terminie 21 dni od daty jej dostarczenia Zamawiającemu, na konto Wykonawcy podane w fakturze.
5. Za dzień zapłaty wynagrodzenia Strony przyjmują datę obciążenia rachunku bankowego Zamawiającego kwotą płatności.
6. W przypadku zwłoki Zamawiającego w zapłacie wynagrodzenia, Wykonawcy przysługują odsetki ustawowe.

§ 14

Wykonawca nie może bez zgody Zamawiającego wyrażonej na piśmie przenieść wierzytelności na osobę trzecią.

§ 15

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   1) w wysokości 10% wartości umowy brutto z tytułu niewykonania lub nienależytego wykonania przedmiotu umowy,
   2) w wysokości 0,5% wartości umowy brutto za każdy dzień zwłoki w realizacji umowy.

2. W przypadku naliczenia kar umownych, o których mowa w ust. 1 pkt 1), Wykonawca zobowiązany jest uregulować naliczoną karę, zgodnie z notą księgową wystawioną przez Zamawiającego.
3. W przypadku naliczenia kar umownych, o których mowa w ust. 1 pkt 2), zostaną one potrącone z wynagrodzenia Wykonawcy.
4. Zamawiający zastrzega sobie prawo do naliczenia kar gwarancyjnych w przypadku przekroczenia czasu naprawy gwarancyjnej w wysokości 0,15% wartości brutto przedmiotu naprawy za każdy dzień opóźnienia w naprawie. Dostarczenie przez Wykonawcę w wymaganym przez Zamawiającego terminie sprzętu zastępczego będzie traktowane jako wykonanie naprawy gwarancyjnej.
5. Zapłata kar umownych nie zwalnia Wykonawcy z obowiązku wykonania przedmiotu umowy lub wykonania naprawy gwarancyjnej.
6. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego przewyższającego wysokość zastrzeżonych kar umownych – na zasadach ogólnych prawa cywilnego, zgodnie z art. 471 Kodeksu cywilnego.

§ 16

Zamawiający zastrzega sobie prawo odstąpienia od umowy na wypadek:

1) niewykonania przedmiotu umowy w zakreślonym terminie,
2) wykonania umowy niezgodnie z jej postanowieniami,
3) wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie zmówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć.

§ 17

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej w postaci pisemnego aneksu pod rygorem nieważności.
2. Niedopuszczalna jest zmiana postanowień umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy.
3. Strony umowy zobowiązują się do niezwłocznego powiadamiania o każdej zmianie adresu, numeru telefonu i telefaksu. Nie stanowi to zmiany umowy.
4. W przypadku niewypełnienia zobowiązania, o którym mowa w ust. 3, pisma wysłane pod adres wskazany w niniejszej umowie uważa się za doręczone skutecznie.

§ 18

Wykonawca zobowiązany jest zachować w tajemnicy wszelkie informacje o Zamawiającym, uzyskane w związku z wykonaniem niniejszej umowy, a w szczególności fakt realizacji

umowy nie może być wykorzystywany przez Wykonawcę do żadnego rodzaju materiałów reklamowych i promocyjnych.

§ 19

Wszelkie spory wynikłe na tle wykonania niniejszej umowy będą rozstrzygały sądy właściwe miejscowo dla Zamawiającego.

§ 20

W sprawach nieuregulowanych niniejszą umową stosuje się przepisy ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych /Dz. U. z 2007r. Nr 223, poz. 1655/ oraz Kodeksu cywilnego.

§ 21

Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, dwóch dla Zamawiającego i jednym dla Wykonawcy.

ZAMAWIAJĄCY WYKONAWCA

Załącznik nr 6

OPIS PRZEDMIOTU ZAMÓWIENIA
ZADANIE I

Serwer nr 1

L.p.	Parametr	Wymagania minimalne
1.	Obudowa	Maksymalnie 2U do instalacji w standardowej szafie RACK 19", dostarczona wraz z szynami
2.	Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów, szyna FSB do 1333 MHz. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym
3.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
4.	Procesor	Quad Core Intel Xeon E5440, 2X6MB Cache,2.8GHz, 1333MHz FSB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
5.	RAM	4 GB DDR2 SDRAM 667MHz FBD, możliwa rozbudowa do 64GB
6.	Zabezpieczenia pamięci RAM	ECC, SDDC (lub równoważny), Online Spare Row, memory mirror
7.	Gniazda PCI	Minimum 3 x PCI-Express z czego minimum 2 x PCI-E x8
8.	Interfejsy sieciowe	Zintegrowana 2 x 10/100/1000 z możliwością obsługi stosu TCP/IP – TOE
9.	Napęd optyczny	Wewnętrzny napęd DVD-ROM
10.	Dyski twarde	2 x 450GB typu HotPlug SAS 3,5" 15krpm, skonfigurowane jako RAID 1, możliwość rozbudowy o cztery dodatkowe dyski twarde
11.	Kontroler RAID	Zintegrowany. Pamięć podręczna minimum 256MB, z podtrzymaniem bateryjnym, możliwe konfiguracje 0, 1, 10, 5, 50, 6, 60
12.	Porty	5 x USB 2.0 z czego 2 na przednim panelu obudowy, 2 na tylnym panelu obudowy i jeden wewnętrzny, 2 x RJ-45, VGA

13.	Video	Zintegrowana karta graficzna
14.	Elementy redundantne HotPlug	Wentylatory, zasilacze
15.	Zasilacze	Redundantne, Hot-Plug o mocy maksymalnie 750W każdy
16.	Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM 1.2
17.	Certyfikaty	Deklaracja zgodności CE. Oferowany model serwera musi znajdować się na liście Windows Server Catalog of Tested Products i posiadać status Certified for Windows dla systemów Windows Server 2008 x86 i Windows Server 2008 x64. Oferowany model serwera musi znajdować się na liście RedHat Certified Hardware i posiadać status Certified (Supported) dla systemów RHEL5-QU1/RHEL4-QU6 i/lub RHEL5-QU1.
18.	Warunki gwarancji dla serwera	• 3 lata na miejscu u klienta. • Możliwość zgłaszania usterek w trybie 24/7/365. • Czas reakcji serwisu w ciągu następnego dnia roboczego. • Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy lub firmy serwisującej, przejmie on na siebie wszelkie zobowiązania związane z serwisem. • W przypadku awarii dysku twardego uszkodzony nośnik pozostaje u Zamawiającego.
19.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim i angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Serwer nr 2

L.p.	Parametr	Wymagania minimalne
1.	Obudowa	Maksymalnie 1U do instalacji w standardowej szafie RACK 19"
2.	Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora, również w technologii quad-core, szyna FSB minimum 1066 MHz lub szybsza. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3.	Procesor	Quad Core Intel Xeon X3360, 2.83GHz, 2x6MB Cache, 1333MHz FSB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
4.	RAM	GB DDR2 Dual Rank, możliwa rozbudowa do 8GB
5.	Zabezpieczenia pamięci RAM	ECC
6.	Gniazda PCI	2 x PCI Express w tym jedno x8
7.	Interfejsy sieciowe	2 x 10/100/1000
8.	Napęd optyczny	Wewnętrzny napęd DVD-ROM
9.	Dyski twarde	2x minimum 250GB SATA, skonfigurowane w RAID1
10.	Video	Zintegrowana karta graficzna
11.	Porty I/O	Wbudowany porty: 2xPS/2, szeregowy, minimum 4 x USB 2.0 wyprowadzone z czego 2 na przednim panelu i dwa z tyłu
12.	Zasilacz	Zasilacz o mocy max. 345W

13.	Szyny montażowe	Statyczne, umożliwiające instalację w szafie 19'', standard Versa
14.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim i angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
15.	Certyfikaty	Deklaracja zgodności CE. Oferowany model serwera musi znajdować się na liście Windows Server Catalog of Tested Products i posiadać status Designed for Windows dla systemów Windows Server 2003 x86 i Windows Server 2003 x64 oraz Certified for Windows dla systemów Windows Server 2008 x86 i Windows Server 2008 x64. Oferowany model serwera musi znajdować się na liście RedHat Certified Hardware i posiadać status Certified (Supported) dla systemu RHEL5-QU1/RHEL4-QU6 i/lub RHEL5-QU1.
16.	Warunki gwarancji dla serwera	• 3 lata na miejscu u klienta. • Możliwość zgłaszania usterek w trybie 24/7/365. • Czas reakcji serwisu do końca następnego dnia roboczego. • Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy lub firmy serwisującej, przejmie on na siebie wszelkie zobowiązania związane z serwisem. • W przypadku awarii dysku twardego uszkodzony nośnik pozostaje u Zamawiającego.

Oprogramowanie

1.	Microsoft Windows Server 2008 Standard (z możliwością zamiennej instalacji Microsoft Windows Serwer 2003 Standard)
2.	Microsoft Exchange Server 2007 Standard
3.	Windows XP Pro z Sp2
4.	Sposób licencjonowania: oprogramowanie ma być licencjonowane w ramach Umowy Licencyjnej Microsoft Open (typu Goverment). Ponadto zaproponowane oprogramowanie musi posiadać taki sposób licencjonowania, który zapewni jego instalację na komputerze (komputerach) inne niż te, na których pierwotnie zainstalowano oprogramowanie, pod warunkiem wcześniejszej deinstalacji z tego komputera (komputerów).

Załącznik nr 7

OPIS PRZEDMIOTU ZAMÓWIENIA
ZADANIE II

Urządzenie zabezpieczające sieć

Lp.	Parametr	Wymagania techniczne
1.	Architektura systemu ochrony	Główne urządzenie ochronne [gateway] nie może posiadać twardego dysku, w zamian ma używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu układu ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy, wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny, pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). Uwaga: Dziennik zdarzeń lub inne działania wymagające systemów dyskowych muszą być realizowane na dedykowanych do tego celu urządzeniach.
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.
3.	Ilość/rodzaj portów	Nie mniej niż **10** portów Ethernet 10/100/1000 Base-TX, oraz możliwość instalacji portów dodatkowego modułu **4** portów 1000 SFP. Nie mniej niż **255** interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę ogniową klasy Stateful Inspection • ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM) • poufność danych - IPSec VPN oraz SSL VPN • ochronę przed atakami - Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających: • kontrolę treści – Web Filter [WF] • kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) • kontrolę pasma oraz ruchu [QoS i Traffic shaping] • kontrolę komunikatorów sieciowych (IM) oraz aplikacji P2P
5.	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: jako router/NAT (3.warstwa ISO-OSI) lub jako most /transparent bridge . Możliwośc wdrożenia urządzenia bez istotnych modyfikacji topologii sieci.

6.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).
7.	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. • Nie mniej niż 3900 sygnatur ataków. • Aktualizacja bazy sygnatur ma się odbywać w sposób automatyczny poprzez sieć lub w sytuacjach awaryjnych ręcznie przy użyciu nośnika. • Możliwość wykrywania anomalii protokołów i ruchu
8.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT.
9.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.
10.	Połączenia VPN	Wymagane nie mniej niż: • Tworzenie połączeń w topologii Site-to-site oraz Client-to-site • Dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki: o firewall o antywirus o web filtering o antyspam • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
11.	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single

		Sign On w środowisku Active Directory bez dodatkowych opłat licencyjnych.
12.	Wydajność	Obsługa nie mniej niż **500 000** jednoczesnych połączeń i **20 000** nowych połączeń na sekundę Przepływność nie mniejsza niż **8 Gb/s** dla ruchu nieszyfrowanego i **6 Gb/s** dla VPN (3DES). Obsługa nie mniej niż **3 000** jednoczesnych tuneli VPN
13.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive
14.	Obudowa	Obudowa ma mieć możliwość zamontowania w szafie 19".
15.	Zasilanie	Zasilanie z sieci 230V/50Hz.
16.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: • haseł statycznych • haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla systemu urządzenie powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
17.	Certyfikaty	Producent musi posiadać następujące certyfikaty: UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus.
18.	Gwarancja i wsparcie	Wsparcie techniczne do zakupionych rozwiązań świadczone w trybie 24/7 (przez 7 dni w tygodniu, 24 godziny na dobę). Wsparcie realizowane przez inżynierów certyfikowanych przez producenta oferowanych rozwiązań. Czas reakcji na zgłoszone problemy nie przekraczający 4 godzin. Wsparcie techniczne obejmujące: pomoc w konfiguracji wspieranych rozwiązań, usuwanie skutków awarii systemu, analiza logów i alertów, pośrednictwo w kontaktach z producentem oferowanego rozwiązania,okresowe wizyty „prewencyjne" realizowane w czasie dogodnym dla Klienta, dostęp do lokalnego portalu wsparcia, oferującego informacje na temat nowych wersji oprogramowania, poprawek, FAQ etc.Przeprowadzenie szkolenia technicznego dla administratorów systemu. Gwarancja na okres min. 12 miesięcy

Urządzenie zbierające i analizujące zdarzenia

Lp.	Parametr	Wymagania techniczne
1.	Architektura systemu	System logowania i raportowania powinien stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i hardware pochodziły od jednego producenta. Urządzenie powinno obsługiwać co najmniej dziesięć urządzeń sieciowych i współpracować z urządzeniem wyszczególnionym w pkt. I.
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
3.	Parametry fizyczne systemu	Nie mniej niż 4 porty Ethernet 10/100 Base-TX Powierzchnia dyskowa - minimum 250 GB
4.	Funkcjonalności podstawowe i uzupełniające	System musi zapewniać: 1. Składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników 2. Możliwość gromadzenia zawartości przesyłanych za pośrednictwem protokołów Web, FTP, email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci 3. Kwarantannę dla współpracujących z nim urządzeń. Kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki. 4. Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących 5. Wyświetlanie nowych logów w czasie rzeczywistym 6. Analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy 7. Analizę podatności stacji w sieci wraz z możliwością raportowania wykrytych luk 8. Export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych)
5.	Aktualizacje sygnatur sprawdzeń	System musi zapewniać: 1. Planowanie aktualizacji bazy sprawdzeń w czasie (Scheduler)
6.	Zarządzanie	System udostępnia: 1. Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH i konsolę szeregową
7.	Zasilanie	• Zasilanie z sieci 230V/50Hz.
8.		Wsparcie techniczne do zakupionych rozwiązań

		świadczone w trybie 24/7 (przez 7 dni w tygodniu, 24 godziny na dobę). Wsparcie realizowane przez inżynierów certyfikowanych przez producenta oferowanych rozwiązań Czas reakcji na zgłoszone problemy nie przekraczający 4 godzin. Wsparcie techniczne obejmujące: pomoc w konfiguracji wspieranych rozwiązań, usuwanie skutków awarii systemu, analiza logów i alertów, pośrednictwo w kontaktach z producentem oferowanego rozwiązania,okresowe wizyty „prewencyjne" realizowane w czasie dogodnym dla Klienta, dostęp do lokalnego portalu wsparcia, oferującego informacje na temat nowych wersji oprogramowania, poprawek, FAQ etc.Przeprowadzenie szkolenia technicznego dla administratorów systemu. Gwarancja na okres min. 12 miesięcy

Załącznik nr 8

OPIS PRZEDMIOTU ZAMÓWIENIA
ZADANIE III
System ochrony poczty

Lp.	wymagania minimalne
1	System musi zapewniać ochronę przed zagrożeniami związanymi z przesyłaniem poczty elektronicznej (wirusy, spam, phishing, niedozwolone treści, etc.), ochronę przeciwko atakom typu Odmowa dostępu do usług (Denial Of Service) oraz logować i zapobiegać enumeracji kont użytkowników chronionej domeny pocztowej (Directory Harvesting Attack).
2	System musi zostać dostarczony w formie kompletnego, zamkniętego rozwiązania sprzętowego.
3	Oferowane rozwiązanie musi być zgodne z obecnie użytkowanym systemem ochrony antywirusowej (instytucja korzysta z f-secura).
4	Urządzenie musi zapewniać wydajność na poziomie minimum 40.000 wiadomości skanowanych w ciągu godziny.
5	Obudowa musi umożliwić montaż w standardowej szafie RACK 19" i posiadać rozmiar 1U.
6	Urządzenie musi posiadać minimum dwa interfejsy sieciowe w standardzie Gigabit BaseT.
7	Pliki systemu operacyjnego, logi, kwarantanna, etc. muszą być przechowywane na dyskach pracujących w standardzie minimum RAID

	1, użyte dyski twarde muszą być tak zainstalowane aby umożliwiać wymianę bez wstrzymywania pracy urządzenia.
8	System w momencie dostarczenia lub po odtworzeniu musi zawierać: - zestaw predefiniowanych reguł i polityk dla wszystkich modułów filtrujących (AV, antyspam, kontrola treści), - powinien zawierać zestaw predefiniowanych raportów.
9	Zarządzanie systemem powinno być możliwe przy użyciu bezpiecznego połączenia https przez przeglądarkę internetową, lub rozwiązanie równoważne.
10	System musi: - pracować jako brama smtp i być niezależnym od rodzaju stosowanych, chronionych serwerów pocztowych, - zapewniać możliwość szyfrowania przesyłek za pomocą protokołu Transport Layer Security w warstwie sieciowej, - umożliwiać korzystanie z zewnętrznych serwerów RBL, - zapewniać wsparcie dla standardu z Sender Policy Framework, - 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, - zapewniać inteligentne rozpoznawanie typów analizowanych załączników, - posiadać lokalną kwarantannę dla zainfekowanych wiadomości, - zapewniać możliwość tworzenia kilku polityk ochrony antywirusowej przydzielanych w oparciu o: adresy IP serwera nadawcy, adres email nadawcy/odbiorcy wiadomości, - zapewniać automatyczną ocenę reputacji źródła przesyłanego mail'a (na podstawie ilości połączeń, procentowej ilości maili z wirusami, procentowej ilości wiadomości zakwalifikowanych jako spam), - posiadać moduł antyspamowy zapewniający analizę statystyczną wiadomości na podstawie minimum 200.000 atrybutów maila, - zapewniać użytkownikom końcowym możliwość zarządzania wiadomościami trafiającymi do ich personalnej kwarantanny, - zapewniać możliwość opcjonalnego uwierzytelniania użytkownika w celu zmian parametrów własnego folderu kwarantanny,

	- umożliwiać następujące operacje na wiadomościach przechowywanych w obszarze kwarantanny: usunięcie wiadomości, przesłanie do odbiorcy, automatyczna zgłoszenie przypadków złej klasyfikacji wiadomości do producenta systemu, - 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, - zapewniać możliwość zdefiniowania wielu administratorów o zróżnicowanych uprawnieniach, - zapewniać automatyczną aktualizację sygnatur antywirusowych, silników skanujących, modułów systemu antyspamowego, oprogramowania i systemu operacyjnego z serwera producenta.
11	Ochrona antywirusowa powinna być realizowana przy pomocy minimum trzech niezależnych silników skanujących.
12	Możliwość definiowania: - różnych sposobów postępowania z zainfekowanymi wiadomościami w zależności od rodzaju wykrytego wirusa, - reguły antyspamowych na poziomie całego urządzenia, grup użytkowników oraz pojedynczych użytkowników, - list zaufanych i blokowanych nadawców przez użytkowników końcowych, - wyglądu kwarantanny końcowego użytkownika zarówno co do jej szaty graficznej (np. możliwość umieszczenia znaku firmowego) jak i treści komunikatów.
13	Aktualizacje sygnatur modułu antywirusowego muszą być dostępny nie rzadziej niż raz na 24 godziny (raz na dobę).
14	Możliwość określenia postępowania z zabezpieczonymi wiadomościami (załączniki chronione hasłem, podpisane wiadomości, etc.).
15	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.
16	Listy użytkowników definiowane lokalnie, możliwość importu użytkowników z serwerów: Active Directory, LDAP, MS Exchange, Lotus Domino oraz plików (tekstowe, csv).
17	Możliwość określania poziomu dostępu i akcji możliwych do wykonania w obrębie kwarantanny dla różnych użytkowników/grup użytkowników.

18	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.
19	Rozbudowany system raportowania zapewniający dostęp do minimum 45 różnych rodzajów graficznych raportów.
20	Możliwość okresowej publikacji wybranych raportów jako strony WWW, przy pomocy wysyłanych automatycznie wiadomości email oraz jako pliki xml.
21	Logowanie na lokalnym dysku twardym lub zewnętrznym serwerze syslog zdarzeń podejmowanych przez filtry oraz zdarzeń dotyczących komunikacji smtp.
22	Możliwość definiowania i przeglądania wielu katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych.
23	Dla wszystkich stworzonych folderów kwarantanny system zapewni możliwość ustawienia maksymalnego czasu przechowywania wiadomości a po jego upływie automatycznie je usunie.
24	System zapewni administratorowi wskazanie folderu/ów, z których wysyłany będzie skrót informacji o wiadomościach przeniesionych do personalnej kwarantanny użytkownika.
25	Możliwość zapisu i odtworzenia konfiguracji.
26	Wszystkie aktualizacje mają być pobierane z jednego miejsca a system komunikować się ze źródłem aktualizacji z częstotliwością narzuconą przez administratora systemu.
27	System zapewni śledzenie historii wykonywania aktualizacji.
28	Producent systemu powinien zapewnić możliwość zakupu aktualizacji systemu jednorazowo na okres roku, dwóch, trzech lat (lub dłużej).
29	Urządzenie powinno być objęte gwarancją "NBD" – czas naprawy nie przekraczający jednego dnia roboczego.
30	Gwarancja na okres min. 12 miesięcy, w przypadku awarii urządzenia dysk/dyski twarde pozostają u zamawiającego
31	Deklaracja zgodności CE