REGIONALNA DYREKCJA
OCHRONY ŚRODOWISKA
w Białymstoku
ul. Dojlidy Fabryczne 23
15-554 Białystok

Białystok, dn.12 stycznia 2016 r.

WOF.261.1.1.2016.AA

Rozpoznanie cenowe o wartości poniżej kwoty określonej w art. 4 pkt 8 ustawy z dn. 29.01.2004 r. Prawo zamówień publicznych (Dz.U. z 2015 poz. 2164)

1. Prowadzący rozpoznanie: Regionalna Dyrekcja Ochrony Środowiska w Białymstoku, ul. Dojlidy Fabryczne 23, 15-554 Białystok.
2. Określenie przedmiotu rozpoznania: zakup 60 licencji oprogramowania antywirusowego wraz z aktualizacją bazy wirusów na potrzeby Regionalnej Dyrekcji Ochrony Środowiska w Białymstoku.

   Szczegółowy opis przedmiotu rozpoznania stanowi załącznik nr 1 do rozpoznania cenowego.
3. Wymagany termin realizacji przedmiotu rozpoznania: **12 miesięcy od daty podpisania umowy.**
4. Kryterium wyboru: 100 % cena.
5. Istotne postanowienia umowy:
   1) Zapłata wynagrodzenia nastąpi przelewem, na wskazany rachunek bankowy Wykonawcy, w terminie do 21 dni od dnia otrzymania faktury VAT przez Zamawiającego.
   2) Regionalna Dyrekcja Ochrony Środowiska w Białymstoku posiada certyfikat Zarządzania Środowiskowego, zgodny z EMAS, nadany w oparciu o Politykę Środowiskową zatwierdzoną przez Regionalnego Dyrektora Ochrony Środowiska w Białymstoku.
   3) Wykonawca oświadcza, że zapoznał się z treścią Polityki Środowiskowej Zamawiającego umieszczonej na jego stronie internetowej pod linkiem: http://www2.bialystok.rdos.gov.pl/media/emas_polityka_srodowiskowa.pdf oraz, że jest świadomy znaczenia zgodności z Polityką Środowiskową przy realizacji postanowień umowy.
6. Osoba upoważniona do kontaktu z wykonawcami: Pan Krystian Kamiński, tel. 857 406 981 wew. 41, e-mail: kkaminski@rdos.gov.pl.
7. Sposób przygotowania zgłoszenia wykonania przedmiotu rozpoznania: ofertę cenową należy złożyć w formie pisemnej, podpisaną przez osobę upoważnioną do reprezentowania firmy, przekazać w formie: osobiście, poprzez złożenie w pok. nr 2, drogą pocztową/faksem/e-mailem na adres: Regionalna Dyrekcja Ochrony Środowiska w Białymstoku, ul. Dojlidy Fabryczne 23, 15-554 Białystok, nr faksu (085) 740 69 82, e-mail: biuro.bialystok@rdos.gov.pl
8. Regionalna Dyrekcja Ochrony Środowiska w Białymstoku posiada certyfikat Systemu Zarządzania Środowiskiem, zgodny z EMAS, nadany w oparciu o Politykę Środowiskową zatwierdzoną przez Regionalnego Dyrektora Ochrony Środowiska w Białymstoku. W związku z tym zaleca się, aby Wykonawcy biorący udział w postępowaniu zapoznali się z treścią Polityki Środowiskowej, zamieszczonej na stronie http://bialystok.rdos.gov.pl/.
9. Termin zgłoszenia wykonania przedmiotu rozpoznania: ofertę cenową należy złożyć do **dnia 19 stycznia 2016 r. godz. 14:00.**

Postępowanie prowadzone jest zgodnie z Regulaminem dokonywania wydatków publicznych o wartości nieprzekraczającej równowartości kwoty określonej w art. 4 pkt 8 ustawy z 29.01.2004 r. Prawo zamówień publicznych w Regionalnej Dyrekcji Ochrony Środowiska w Białymstoku

Z up. Regionalnego Dyrektora
Ochrony Środowiska w Białymstoku
Beata Bezubik
Zastępca Dyrektora

.....
(*podpis zamawiającego*)

Zał.:
1) Szczegółowy opis przedmiotu rozpoznania.
2) Formularz oferty cenowej.

Niniejsze rozpoznanie cenowe nie stanowi zobowiązania Regionalnej Dyrekcji Ochrony Środowiska w Białymstoku do udzielenia zamówienia. Zamawiający dokona wyboru oferty najkorzystniejszej na warunkach określonych w ogłoszeniu i powiadomi o przyjęciu oferty wybranego wykonawcę

Załącznik nr 1
do rozpoznania cenowego

Szczegółowy opis przedmiotu rozpoznania

1. Przedmiotem zamówienia jest dostawa licencji wielostanowiskowej na oprogramowanie antywirusowe wraz z aktualizacją bazy wirusów na potrzeby Regionalnej Dyrekcji Ochrony Środowiska w Białymstoku.
2. Zamawiający obecnie posiada licencję wielostanowiskową oprogramowania ESET Endpoint Antivirus Suite na 60 stanowisk.
3. Dostarczone oprogramowanie ma chronić systemy użytkowane przez Zamawiającego:
   1) 58 fizycznych stacji roboczych z systemem Windows 7/8.1/10 (x64 oraz x86),
   2) 2 wirtualne serwery plików z systemem Windows Server 2008 i 2012, działające na hoście Microsoft Hyper-V 3.0.
4. ***Wymagania wspólne dla ochrony stacji roboczych oraz serwerów plików:***
   1) Ochrona antywirusowa i antyspyware w czasie rzeczywistym.
   2) Możliwość skanowania z wykorzystaniem analizy heurystycznej oraz sygnatur wirusów.
   3) Możliwość wykonania skanowania według harmonogramu (codziennie o określonej godzinie lub w wybrane dni tygodnia) oraz na żądanie.
   4) Automatyczne skanowanie systemu w trakcie bezczynności chronionego urządzenia.
   5) Możliwość aktualizacji bazy wirusów z Internetu lub z lokalnego serwera aktualizacji oraz aktualizacji bazy w trybie offline.
   6) Zdalna instalacja aplikacji, uruchamianie zadań, zbieranie logów.
   7) Możliwość definiowania wykluczeń skanowania na podstawie rozszerzenia plików oraz według określonej ścieżki do folderu lub pliku.
   8) Producent udostępnia gotowy obraz płyty lub narzędzie do przygotowania awaryjnego nośnika CD/DVD/USB, z którego będzie możliwe uruchomienie zainfekowanego urządzenia w celu przeskanowanie i usunięcia wirusów.
   9) Możliwość przeniesienia zainfekowanych plików do kwarantanny.
   10) Kontrola i powiadomienia o brakujących krytycznych aktualizacjach systemu operacyjnego.
   11) Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, zadań skanowania, aktualizacji baz wirusów i samego oprogramowania.
5. ***Wymagania dodatkowe dotyczące ochrony stacji roboczych:***
   1) Skanowanie protokołów: HTTP, POP3, IMAP.
   2) Ochrona programów pocztowych: Microsoft Outlook (2007, 2010, 2013, 2016) oraz Mozilla Thunderbird 38.
   3) Możliwość automatycznego skanowania nośników wymiennych (pendrive, CD/DVD, dyski USB, karty pamięci) po podłączeniu do komputera.
   4) Automatyczne wykrywanie i usuwanie innego oprogramowania antywirusowego podczas instalacji.
   5) GUI w polskiej wersji językowej.
6. ***Wymagania dotyczące serwera zarządzającego:***
   1) Serwer dostępny, jako Virtual Appliance dla hosta Hyper-V lub jako aplikacja do zainstalowania w systemie Windows Server 2008/2012.

2) Konsola serwera dostępna przez przeglądarkę www lub jako aplikacja do zainstalowania w systemie Windows 7/8.1/10 64bit.
3) Integracja z domeną Active Directory umożliwiająca logowanie administratora do konsoli z wykorzystaniem poświadczeń domenowych oraz widok struktury lasu (OU oraz grupy domenowe).
4) Zdalna instalacja oprogramowania antywirusowego na stacjach roboczych i serwerach plików.
5) Pełna administracja zdalnymi klientami za pomocą konsoli administracyjnej (zarządzanie wszystkimi ustawieniami programu antywirusowego, ustanawianie polityk bezpieczeństwa, zbieranie logów, uruchamianie zadań skanowania).
6) Możliwość wyświetlenia informacji dotyczących zarządzanego urządzenia, takich jak: wersja programu antywirusowego i bazy wirusów, aktualna konfiguracja programu, wyniki skanowania, wykryte zagrożenia.
7) Wbudowane narzędzie diagnostyczne generujące szczegółowy raport dotyczący zarządzanego urządzenia zawierający: listę zainstalowanych aplikacji oraz usług systemowych, informacje o systemie operacyjnym, sprzęcie, aktywnych procesach i połączeniach.
8) Centralne zarządzanie kwarantanną zarządzanych urządzeń.
9) Możliwość przywrócenia lub pobrania zainfekowanego pliku z kwarantanny stacji klienckiej.
10) Automatyczne powiadomienia o zagrożeniach wykrytych na stacjach roboczych i serwerach (email, wpis do dziennika systemu Windows oraz do konsoli serwera zarządzającego).
11) Tworzenie raportów zawierających statystyki dotyczące wykrytych zagrożeń.
12) Możliwość konfiguracji, jako wewnętrzny serwer aktualizacji pobierający aktualizacje sygnatur wirusów z serwerów producenta w celu dystrybucji do stacji klienckich.
13) Identyfikacja niezarządzanych maszyn w domenie Windows Active Directory.
14) Możliwość samodzielnego logicznego grupowania klientów jak również wykorzystania grup zdefiniowanych w domenie Active Directory oraz przypisywania do grup określonych zasad bezpieczeństwa.

7. Termin realizacji przedmiotu rozpoznania: **12 miesięcy od daty podpisania umowy.**