### ZAPYTANIE OFERTOWE

**ZAMAWIAJĄCY:**

**Powiatowy Urząd Pracy w Gryfinie**

**ul. Łużycka 55**

**74-100 Gryfino**

ZAPRASZA DO ZŁOŻENIA OFERTY W POSTĘPOWANIU PROWADZONYM

NA ZASADACH OBOWIĄZUJĄCYCH PRZY ZAMÓWIENIACH PONIŻEJ KWOTY

30 000 EURO

na

**zakup wznowień licencji, wsparć i urządzeń sieciowych dla Powiatowego Urzędu Pracy w Gryfinie**

**KOD CPV 48760000-3 Pakiet oprogramowania do ochrony antywirusowej**

**KOD CPV 72611000-6 Usługi w zakresie wsparcia technicznego**

**KOD CPV 72253200-5 Usługi w zakresie wsparcia systemu**

**KOD CPV 48214000-1 Pakiety oprogramowania do sieciowego systemu operacyjnego**

**KOD CPV 32422000-7 Elementy składowe sieci**

**KOD CPV 32420000-3 Urządzenia sieciowe**

**KOD CPV 32415000-5 Sieć Ethernet**

**KOD CPV 32428000-9 Modernizacja sieci**

Podstawa prawna: Ustawa z dnia 29.01.2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2015, poz. 2164 z późn. zm.) zwana dalej ustawą PZP.

ROZDZIAŁ I Opis przedmiotu zamówienia

Przedmiotem zamówienia jest **zakup wznowień licencji, wsparć i urządzeń sieciowych dla Powiatowego Urzędu Pracy w Gryfinie**

**KOD CPV 48760000-3 Pakiet oprogramowania do ochrony antywirusowej**

**KOD CPV 72611000-6 Usługi w zakresie wsparcia technicznego**

**KOD CPV 72253200-5 Usługi w zakresie wsparcia systemu**

**KOD CPV 48214000-1 Pakiety oprogramowania do sieciowego systemu operacyjnego**

**KOD CPV 32422000-7 Elementy składowe sieci**

**KOD CPV 32420000-3 Urządzenia sieciowe**

**KOD CPV 32415000-5 Sieć Ethernet**

**KOD CPV 32428000-9 Modernizacja sieci**

Zakres zamówienia obejmować będzie dostarczenie:

1. Dostarczenie fabrycznie nowego i zapakowanego urządzenia sieciowego klasy UTM ((ang. unified threat management) – wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia) FortiGate 91E lub równoważnego. Urządzenie musi mieć pełna kompatybilność z pozostałymi produktami marki FortiNet w tym FortiMail i FortiAP ze względu na posiadane już przez Zamawiającego produkty. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa obsługujących Zamawiającego, Wykonawca zapewni wszystkie poniższe funkcjonalności:

1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
5. System realizujący funkcję Firewall powinien dysponować minimum 16 portami Ethernet 10/100/100 BaseTX
6. Możliwość tworzenia min 254 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
7. W zakresie Firewall’a obsługa nie mniej niż 1 milion jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę
8. Przepustowość Firewall’a: nie mniej niż 4 Gbps
9. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 100 GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku do poszczególnych lokalizacji musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
10. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:

* kontrola dostępu - zapora ogniowa klasy Stateful Inspection
* ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS).
* poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
* ochrona przed atakami - Intrusion Prevention System [IPS]
* kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
* kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
* kontrola pasma oraz ruchu [QoS, Traffic shaping]
* Kontrola aplikacji oraz rozpoznawanie ruchu P2P
* Możliwość analizy ruchu szyfrowanego protokołem SSL
* Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji

1. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:

* Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
* Praca w topologii Hub and Spoke oraz Mesh
* Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

1. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.
2. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall’a, Antywirus’a, IPS’a, Web Filter’a.
3. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
4. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
5. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
6. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
7. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
8. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
9. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
10. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
11. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
* haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
* haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
* Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.

1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

* ICSA dla funkcjonalności SSLVPN, IPS, Antywirus
* ICSA lub EAL4 dla funkcjonalności Firewall

1. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
2. Serwisy i licencje

* Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 12 miesięcy.

1. Gwarancja oraz wsparcie:

* **Gwarancja:** System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.
* **Gwarancja:** System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym. Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię 8x5 (należy podać numer infolinii).

1. Dostarczenie fabrycznie nowego i zapakowanego urządzenia sieciowego klasy UTM ((ang. unified threat management) – wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia) FortiWIFI 50E lub równoważnego. Urządzenie musi mieć pełna kompatybilność z pozostałymi produktami marki FortiNet w tym FortiMail i FortiAP ze względu na posiadane już przez Zamawiającego produkty. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa obsługujących Zamawiającego, Wykonawca zapewni wszystkie poniższe funkcjonalności:

1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
5. System realizujący funkcję Firewall powinien dysponować minimum 5 portami Ethernet 10/100/100 BaseTX
6. Możliwość tworzenia min 254 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
7. W zakresie Firewall’a obsługa nie mniej niż 1 milion jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę
8. Przepustowość Firewall’a: nie mniej niż 2,5 Gbps
9. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:

* kontrola dostępu - zapora ogniowa klasy Stateful Inspection
* ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS).
* poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
* ochrona przed atakami - Intrusion Prevention System [IPS]
* kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
* kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
* kontrola pasma oraz ruchu [QoS, Traffic shaping]
* Kontrola aplikacji oraz rozpoznawanie ruchu P2P
* Możliwość analizy ruchu szyfrowanego protokołem SSL
* Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji

1. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:

* Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
* Praca w topologii Hub and Spoke oraz Mesh
* Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

1. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.
2. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall’a, Antywirus’a, IPS’a, Web Filter’a.
3. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
4. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
5. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
6. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
7. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
8. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
9. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
10. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
11. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
* haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
* haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
* Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.

1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

* ICSA dla funkcjonalności SSLVPN, IPS, Antywirus
* ICSA lub EAL4 dla funkcjonalności Firewall

1. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
2. Serwisy i licencje

* Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 12 miesięcy.

1. Gwarancja oraz wsparcie:

* **Gwarancja:** System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.
* **Gwarancja:** System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym. Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię 8x5 (należy podać numer infolinii).

1. Dostarczenie dwóch fabrycznie nowych i zapakowanych urządzeń sieciowego typu access point – wielofunkcyjne bezprzewodowe punkty dostępowe FortiAP 221C lub równoważnych. Urządzenie musi mieć pełna kompatybilność z pozostałymi produktami marki FortiNet w tym FortiMail i FortiGate ze względu na posiadane już przez Zamawiającego produkty. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej. Urządzenia muszą posiadać możliwość pełnej kompatybilności z urządzeniami klasy UTM dostarczonymi w punkcie 1 i 2 zamówienia.
2. Serwisy i licencje

* Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 36 miesięcy.

1. Gwarancja oraz wsparcie:

* **Gwarancja:** System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.
* **Gwarancja:** System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym. Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię 8x5 (należy podać numer infolinii).

1. Dostarczenie 100 licencji odnowień dla pakietu oprogramowania antywirusowego ESET Suite Antyvirus na okres jednego roku.
2. Dostarczenie licencji rocznej na wsparcie i aktualizację pakietu VMware vSphere Essential Kit Plus
3. Wdrożenie obejmujące:
   1. Instalację urządzeń w szafie typu rack,,
   2. Konfiguracja połączenia z istniejącą infrastrukturą w tym:

* Przeniesienie istniejących protokołów i ustawień sieciowych typu vpn, vlan do nowego urządzenia,
* Dostosowanie polityk do nowego urządzenia
  1. Konfiguracja urządzeń pod kontem protokołu sieciowego 802.1x
  2. Testy połączeń typu VPN, logowania użytkowników AD.
  3. Sprawdzenie sieci pod względem podatności na zagrożenia z zewnątrz.

Pozostałe wymagania:

.

1. Wykonawca dostarczy na własny koszt zamówienie do siedziby zamawiającego:

Powiatowy Urząd Pracy w Gryfinie

Ul. Łużycka 55

74-100 Gryfino

w godzinach pracy urzędu 7:30-15:30

oraz jego Filii:

ul. Dworcowa 3

74-500 Chojna

1. Urządzenia muszą być dostarczone przez oficjalny kanał dystrybucyjny w Polsce.
2. Urządzenia musza być dostarczone z pełną dokumentacją techniczną.
3. Licencje muszą być przekazane w postaci elektronicznej na wskazany przez zamawiającego adres poczty elektronicznej.

ROZDZIAŁ II Termin wykonania zamówienia

Czas realizacji - 10 dni roboczych od dnia przyjęcia zlecenia. Przewidywany termin dokonania zlecenia - grudzień 2016r.

**ROZDZIAŁ III Warunki udziału w postępowaniu**

O udzielenie zamówienia publicznego mogą ubiegać się wykonawcy którzy:

1. Nie podlegają wykluczeniu z postępowania o udzielenie zamówienia publicznego o którym mowa

w art. 24 ust.1 pkt 12-23 ustawy PZP.

1. Spełniają określone przez zamawiającego warunki udziału w postępowaniu dotyczące:

**2.1. Zdolności technicznej lub zawodowej dotyczącej Wykonawcy:**

Wykonawca składający ofertę musi posiadać doświadczenie w zakresie realizacji dostaw objętych przedmiotem zamówienia - oświadczyć, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie zrealizował co najmniej 3 dostawy przedmiotów opisanych w zamówieniu.

**2.2. Zdolności technicznej lub zawodowej dotyczącej osób skierowanych przez zamawiającego do realizacji zamówienia:**

Wykonawca składający ofertę musi dysponować osobami, które będą uczestniczyć w wykonaniu zamówienia, posiadając kwalifikacje zawodowe i doświadczenie zawodowe adekwatnym do przedmiotu zamówienia.

|  |
| --- |
| ROZDZIAŁ IV Wykaz oświadczeń i dokumentów, jakie mają dostarczyć wykonawcy w celupotwierdzenia spełniania warunków udziału w postępowaniu |

1. Wykonawca jest zobowiązany do złożenia następujących dokumentów:
   1. Oświadczenie wykonawcy o spełnianiu warunków udziału w postępowaniu na załączniku Nr 2
   2. Oświadczenie wykonawcy dotyczące przesłanek do wykluczenia z postępowania na załączniku Nr 3

|  |
| --- |
| ROZDZIAŁ V Opis sposobu przygotowania oferty |

***Oferta wykonawcy***

1. Oferta wraz z załącznikami musi być podpisana przez osobę upoważnioną do reprezentowania wykonawcy
2. Jeżeli osoba podpisująca ofertę działa na podstawie pełnomocnictwa to pełnomocnictwo to musi w swej treści jednoznacznie wskazywać uprawnienie do podpisania oferty. Pełnomocnictwo to musi zostać dołączone do oferty i musi być złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem.
3. Dokumenty składające się na ofertę mogą być złożone w oryginale, kserokopii potwierdzonej za zgodność z oryginałem przez wykonawcę lub drogą elektroniczną na adres podany w rozdziale VII zapytania.
4. Na **ofertę** składają się:
5. Formularz ofertowy według wzoru w **załączniku nr 1** do zapytania ofertowego
6. Oświadczenie wykonawcy o spełnianiu warunków udziału w postępowaniu na **załączniku nr 2** do zapytania ofertowego
7. Oświadczenie wykonawcy dotyczące przesłanek do wykluczenia z postępowania na **załączniku nr 3** do zapytania ofertowego
8. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

|  |
| --- |
| **ROZDZIAŁ VI Kryteria wyboru oferty najkorzystniejszej** |

1. Przy wyborze oferty będą brane następujące kryteria:

**Cena - waga kryterium – 100%**

|  |
| --- |
| ROZDZIAŁ VII Miejsce i termin składania ofert |

Ofertę należy złożyć do dnia **13.12.2016 r. do godz. 13:00** w formie elektronicznej na dołączonym formularzu ofertowym (załącznik nr 1 do niniejszego zapytania ofertowego wraz z załącznikiem nr 2 i 3) na adres e-mail: [mdworzynski@pupgryfino.com.pl](mailto:mdworzynski@pupgryfino.com.pl) lub osobiście w siedzibie Zamawiającego, tj. Powiatowy Urząd Pracy w Gryfinie, ul. Łużycka 55, 74-100 Gryfino. Oferty złożone po terminie nie będą rozpatrywane.

*Wzór*

|  |
| --- |
| Załącznik nr 1 FORMULARZ OFERTOWY |

Nazwa przedmiotu zamówienia :

Przedmiotem zamówienia jest **zakup wznowień licencji, wsparć i urządzeń sieciowych dla Powiatowego Urzędu Pracy w Gryfinie**

**KOD CPV 48760000-3 Pakiet oprogramowania do ochrony antywirusowej**

**KOD CPV 72611000-6 Usługi w zakresie wsparcia technicznego**

**KOD CPV 72253200-5 Usługi w zakresie wsparcia systemu**

**KOD CPV 48214000-1 Pakiety oprogramowania do sieciowego systemu operacyjnego**

**KOD CPV 32422000-7 Elementy składowe sieci**

**KOD CPV 32420000-3 Urządzenia sieciowe**

**KOD CPV 32415000-5 Sieć Ethernet**

**KOD CPV 32428000-9 Modernizacja sieci**

Nazwa i adres wykonawcy

………………………………………………………………………………………………………………

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

REGON ……………………………………………. PKD ……………………………………...……….

NIP ……………………………………………………………………………..………………......….......

Numer rachunku bankowego wykonawcy …………………………………………..............................................………………………….....………

Imię i nazwisko osoby/osób uprawnionej do reprezentowania wykonawcy ( podpisania umowy o realizację zamówienia) ……………………………………………………………………...................…

Telefon/Fax/e-mail.......................................................................................................................................

**Oświadczam, iż zobowiązuję się do:**

1. Dostarczenia fabrycznie nowego i zapakowanego urządzenia sieciowego klasy UTM ((ang. unified threat management) – wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia) FortiGate 91E lub równoważnego. Urządzenie musi mieć pełna kompatybilność z pozostałymi produktami marki FortiNet w tym FortiMail i FortiAP ze względu na posiadane już przez Zamawiającego produkty. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Produkt zamówienia będzie spełniał wszystkie parametry zawarte w opisie przedmiotu zamówienia – Rozdział 1 zapytania.
2. Dostarczenia fabrycznie nowego i zapakowanego urządzenia sieciowego klasy UTM ((ang. unified threat management) – wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia) FortiWIFI 50E lub równoważnego. Urządzenie musi mieć pełna kompatybilność z pozostałymi produktami marki FortiNet w tym FortiMail i FortiAP ze względu na posiadane już przez Zamawiającego produkty. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Produkt zamówienia będzie spełniał wszystkie parametry zawarte w opisie przedmiotu zamówienia – Rozdział 1 zapytania.
3. Dostarczenia dwóch fabrycznie nowych i zapakowanych urządzeń sieciowego typu access point – wielofunkcyjne bezprzewodowe punkty dostępowe FortiAP 221C lub równoważnych. Urządzenie musi mieć pełna kompatybilność z pozostałymi produktami marki FortiNet w tym FortiMail i FortiGate ze względu na posiadane już przez Zamawiającego produkty. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej. Urządzenia muszą posiadać możliwość pełnej kompatybilności z urządzeniami klasy UTM dostarczonymi w punkcie 1 i 2 zamówienia. Produkty zamówienia będą spełniał wszystkie parametry zawarte w opisie przedmiotu zamówienia – Rozdział 1 zapytania.
4. Dostarczenia 100 licencji odnowień dla pakietu oprogramowania antywirusowego ESET Suite Antyvirus na okres jednego roku.
5. Dostarczenia licencji rocznej na wsparcie i aktualizację pakietu VMware vSphere Essential Kit Plus.
6. Wdrożenia obejmującego:
7. Instalację urządzeń w szafie typu rack,,
8. Konfiguracje połączenia z istniejącą infrastrukturą w tym:

* Przeniesienie istniejących protokołów i ustawień sieciowych typu vpn, vlan do nowego urządzenia,
* Dostosowanie polityk do nowego urządzenia

1. Konfiguracje urządzeń pod kontem protokołu sieciowego 802.1x
2. Testy połączeń typu VPN, logowania użytkowników AD.
3. Sprawdzenie sieci pod względem podatności na zagrożenia z zewnątrz.

Pozostałe wymagania:

1. Wykonawca dostarczy na własny koszt zamówienie do siedziby zamawiającego:

Powiatowy Urząd Pracy w Gryfinie

Ul. Łużycka 55

74-100 Gryfino

w godzinach pracy urzędu 7:30-15:30

oraz jego Filii:

ul. Dworcowa 3

74-500 Chojna

1. Urządzenia muszą być dostarczone przez oficjalny kanał dystrybucyjny w Polsce.
2. Urządzenia musza być dostarczone z pełną dokumentacją techniczną.
3. Licencje muszą być przekazane w postaci elektronicznej na wskazany przez zamawiającego adres poczty elektronicznej.

………………., dnia …………… …………………………………………………….

osoba uprawniona do reprezentowania wykonawcy

**OFERTA CENOWA**

Łączna cena za realizację całości zamówienia …………………….. zł brutto

………………., dnia …………… …………………………………………………….

osoba uprawniona do reprezentowania wykonawcy

|  |
| --- |
| Załącznik nr 2 Oświadczenie o spełnianiu warunków udziału w postępowaniu |

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

(pieczęć wykonawcy)

**OŚWIADCZENIE WYKONAWCY**

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

**Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. „**Zakup wznowień licencji, wsparć i urządzeń sieciowych dla Powiatowego Urzędu Pracy w Gryfinie”**,prowadzonego przez Powiatowy Urząd Pracy w Gryfinie*,* działając w imieniu i na rzecz *(nazwa firmy i adres wykonawcy)*

………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………

oświadczam, co następuje:

**INFORMACJA DOTYCZĄCA WYKONAWCY:**

Wykonawca, którego reprezentuję spełnia samodzielnie/polegając na zasobach innych podmiotów\* warunki udziału w postępowaniu określone w Zapytaniu ofertowym dotyczące:

1. **Zdolności technicznej lub zawodowej dotyczącej Wykonawcy:**

Wykonawca składający ofertę musi posiadać doświadczenie w zakresie realizacji dostaw objętych przedmiotem zamówienia - oświadczyć, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie zrealizował co najmniej 3 dostawy przedmiotów opisanych w zamówieniu..

1. **Zdolności technicznej lub zawodowej dotyczącej osób skierowanych przez zamawiającego do realizacji zamówienia:**

Wykonawca składający ofertę musi dysponować osobami, które będą uczestniczyć w wykonaniu zamówienia, posiadając kwalifikacje zawodowe i doświadczenie zawodowe adekwatnym do przedmiotu zamówienia.

………………….. dnia …………… .............................................................................................. (podpis osoby uprawnionej do reprezentacji wykonawcy )

**INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW**:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w Zapytaniu ofertowym polegam na zasobach następującego/ych podmiotu/ów *(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu oraz załączyć dokument o oddaniu do dyspozycji odpowiednich zasobów ):*

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

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

w następującym zakresie: …………………………………………………………………………….………………

…………………………………………………………………………………………………………………………

………………….. dnia …………… .............................................................................................. (podpis osoby uprawnionej do reprezentacji wykonawcy )

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

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

………………….. dnia …………… .............................................................................................. (podpis osoby uprawnionej do reprezentacji wykonawcy )

|  |
| --- |
| Załącznik nr 3 Oświadczenie dotyczące przesłanek wykluczenia z postępowania |

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

(pieczęć wykonawcy)

**OŚWIADCZENIE WYKONAWCY**

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

**Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.„ **Zakup wznowień licencji, wsparć i urządzeń sieciowych dla Powiatowego Urzędu Pracy w Gryfinie”**prowadzonego przez Powiatowy Urząd Pracy w Gryfinie*,* działając w imieniu i na rzecz *(nazwa firmy i adres wykonawcy)*

………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………

oświadczam, co następuje:

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:**

Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust 1 pkt 12-23 ustawy Pzp.

…………….……. *(miejscowość),* dnia …………………. r. …………………………………………

*(podpis)*

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

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

…………….……. *(miejscowość),* dnia …………………. r. …………………………………………

*(podpis)*

**OŚWIADCZENIE DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:**

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby powołuję  się  w  niniejszym  postępowaniu,  tj.: …………………………………………………………… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)* nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

…………….……. *(miejscowość),* dnia …………………. r. …………………………………………

*(podpis)*

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

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

…………….……. *(miejscowość),* dnia …………………. r. …………………………………………

*(podpis)*