Załącznik nr 1 do siwz
Załącznik nr 1 do umowy nr…….
z dnia……

Opis przedmiotu zamówienia

Etap 1 - Uruchomienie dostępu do szerokopasmowego Internetu w jednostkach podległych Powiatowi Skarżyskiemu

Wykonanie w terminie **4 tygodni od dnia podpisania umowy**
Parametry techniczne:

Wykonawca zapewni przyłączenie do sieci Internetowej jednostkom podległym Powiatowi Skarżyskiemu (6 lokalizacji) oraz zapewni dostęp do sieci Internet poprzez zastosowanie dostępnych i osiągalnych rozwiązań technologicznych (systemy przewodowe, systemy bezprzewodowe) zgodnie z najlepszymi obowiązującymi normami i praktykami.

Internet należy udostępnić dla urządzeń pracujących w sieci komputerowej w jednostkach podległych powiatowi skarżyskiemu (która została stworzona na potrzeby projektu pn. Przeciwdziałanie wykluczeniu cyfrowemu w Powiecie Skarżyskim)

Lokalizacje do których należy podłączyć dostęp do Internetu:

1. Powiatowe Centrum Pomocy Rodzinie - Plac Floriański 1, Skarżysko-Kamienna
2. Powiatowy Środowiskowy Dom Samopomocy - ul. Tysiąclecia 22, Skarżysko-Kamienna
3. Dom Pomocy Społecznej - ul. Sporna 6, Skarżysko-Kamienna
4. Zespół Placówek Edukacyjno-Wychowawczych - ul. Szkolna 15, Skarżysko-Kamienna
5. Zespół Placówek Opieki, Wychowania i Interwencji Kryzysowej „Przystań" - ul. Rejowska 53, Skarżysko-Kamienna
6. Powiatowe Centrum Rozwoju Edukacji (dawniej Poradnia Psychologiczno-Pedagogiczna) - Plac Floriański 1, Skarżysko-Kamienna

Przedmiot zamówienia obejmuje: podłączenie, konfigurację oraz aktywację szerokopasmowego Internetu wraz z dostawą i instalacją niezbędnych urządzeń/zestawów umożliwiających korzystanie z oferowanej usługi dostępowej dla sześciu jednostek podległych Powiatowi Skarżyskiemu.

Etap 2 – Dostawa wraz z konfiguracją i uruchomieniem urządzeń sieciowych w jednostkach podległych Powiatowi Skarżyskiemu w celu uzyskania komunikacji ze sprzętem oraz kontrolerem sieci bezprzewodowej, które znajdują się w jednostkach podległych (zakupionych wcześniej w ramach projektu pn. Przeciwdziałanie wykluczeniu cyfrowemu w Powiecie Skarżyskim) – 6 szt.

Wykonanie w terminie **4 tygodni od dnia podpisania umowy**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 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 wykonawca zapewni wszystkie poniższe funkcjonalności:

1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
2. Elementy systemu przenoszące ruch użytkowników powinny dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent
3. System realizujący funkcję Firewall powinien dysponować minimum 5 interfejsami miedzianymi Ethernet 10/100/1000
4. Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
5. W zakresie Firewall'a obsługa nie mniej niż 150tys jednoczesnych połączeń oraz 3 tys. nowych połączeń na sekundę.
6. 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:
    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    b. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). System kontroli AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    c. Poufność danych - IPSec VPN oraz SSL VPN
    d. Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
    e. Kontrola stron Internetowych – Web Filter [WF]
    f. Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
    g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
    h. Możliwość analizy ruchu szyfrowanego SSL'em
    i. Ochrona przed wyciekiem poufnej informacji (DLP)
7. Wydajność systemu Firewall min 500 Mbps

8. Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 20Mbps
9. Wydajność ochrony przed atakami (IPS) min 100 Mbps.
10. Wydajność IPSEC VPN, nie mniej niż 200 Mbps
11. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    a. Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
    b. Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
    c. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    d. Praca w topologii Hub and Spoke oraz Mesh
    e. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
    f. Obsługa ssl vpn w trybach portal oraz tunel
12. Rozwiązanie powinno zapewniać: routing statyczny oraz obsługę Policy Routingu
13. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
14. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń
15. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
16. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
17. Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 6000 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.
18. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
19. Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 50 kategorii. W ramach filtra powinny być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
20. Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

21. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
    d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
22. Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall powinien posiadać certyfikat ICSA dla rozwiązań kategorii Network Firewall
23. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Etap 3 - Koszt łącza internetowego w jednostkach podległych Powiatowi Skarżyskiemu w okresie od dnia uruchomienia dostępu do dnia 30.09.2015r.

Świadczenie usługi: od dnia podłączenia do **30.09.2015**

Szczegóły:

- Stały dostęp do sieci Internet **(24 godziny na dobę, 7 dni w tygodniu)**
- **Brak limitów** wysyłania i pobierania danych
- Dostępność usługi na **poziomie 99%**
- **Parametry Internetu:**
  Transfer do komputera (down) – **8 Mb/s**
  Transfer od komputera (up) – **2 Mb/s**
- Dostęp do Internetu z punktu widzenia Zamawiającego musi działać bezobsługowo, co oznacza, że po odłączeniu zasilania i ponownym jego odłączeniu musi być gotowy do pracy i umożliwić realizację usługi korzystania z Internetu
- Dodatkowe niezbędne urządzenia / zestawy do prawidłowego działania usługi dostarczy Wykonawca

Serwis:

1. Wykonawca odpowiada nieodpłatnie za przywrócenie sprawności łącza (dostępu do Internetu i rozwiązanie zaistniałych problemów) w czasie nie dłuższym **niż 2 dni robocze** od chwili ich zgłoszenia.

2. Rozwiązanie zaistniałych problemów może nastąpić w sposób bezpośredni (wizyta serwisanta) lub jeśli będzie to możliwe w sposób zdalny.
3. Wykonawca będzie zobowiązany do usuwania usterek związanych tylko i wyłącznie z dostępem do sieci Internet.
4. Wykonawca ma obowiązek telefonicznego informowania Zamawiającego o wystąpieniu awarii oraz planowanych przerwach w dostępie do usługi i przewidywanym czasie jej usunięcia.
5. Wykonawca zapewni alarmowy kontakt z serwisem: telefonicznie **przez 5 dni w tygodniu** (od poniedziałku do piątku) **w godz. 8.00-17.00.**
6. W celu zapewnienia ciągłości dostępu do Internetu Wykonawca zobowiązuje się do konfiguracji, utrzymania, aktualizacji, naprawy, serwisowania i wymiany urządzeń / zestawów /oprogramowania będących przedmiotem umowy.

W jednostkach podległych Powiatowi Skarżyskiemu aktualnie znajduje się następujący sprzęt komputerowy zakupiony wcześniej w ramach projektu pn. Przeciwdziałanie wykluczeniu cyfrowemu w Powiecie Skarżyskim:

1) Powiatowe Centrum Pomocy Rodzinie - Plac Floriański 1, Skarżysko-Kamienna
   - 3 Komputery przenośne Dell Latitude 3540, system operacyjny MS Windows, pakiet biurowy MS Office MOLP, program antywirusowy GData AV
   - Osprzęt sieciowy LAN Extreme Networks AP4022i int ant EU
2) Powiatowy Środowiskowy Dom Samopomocy - ul. Tysiąclecia 22, Skarżysko-Kamienna
   - 4 Komputery przenośne Dell Latitude 3540, system operacyjny MS Windows, pakiet biurowy MS Office MOLP, program antywirusowy GData AV
   - Osprzęt sieciowy LAN Extreme Networks AP4022i int ant EU
3) Dom Pomocy Społecznej - ul. Sporna 6, Skarżysko-Kamienna
   - 3 Komputery przenośne Dell Latitude 3540, system operacyjny MS Windows, pakiet biurowy MS Office MOLP, program antywirusowy GData AV
   - Osprzęt sieciowy LAN Extreme Networks AP4022i int ant EU
4) Zespół Placówek Edukacyjno-Wychowawczych - ul. Szkolna 15, Skarżysko-Kamienna
   - 6 Komputerów przenośnych Dell Latitude 3540, system operacyjny MS Windows, pakiet biurowy MS Office MOLP, program antywirusowy GData AV
   - Osprzęt sieciowy LAN Extreme Networks AP4022i int ant EU
5) Zespół Placówek Opieki, Wychowania i Interwencji Kryzysowej „Przystań" - ul. Rejowska 53, Skarżysko-Kamienna
   - 4 Komputery przenośne Dell Latitude 3540, system operacyjny MS Windows, pakiet biurowy MS Office MOLP, program antywirusowy GData AV
   - Osprzęt sieciowy LAN Extreme Networks AP4022i int ant EU
6) Powiatowe Centrum Rozwoju Edukacji (dawniej Poradnia Psychologiczno-Pedagogiczna) - Plac Floriański 1, Skarżysko-Kamienna
   - 10 Komputerów przenośnych Dell Latitude 3540, system operacyjny MS Windows, pakiet biurowy MS Office MOLP, program antywirusowy GData AV

- Serwer z oprogramowaniem i UPS Dell PowerEdge T320 TPM, MS Windows Server, Pakiet Novell Open Workgroup Suite, UPS GTEC AP160N-3K
- Osprzęt sieciowy LAN Extreme Networks AP4022i int ant EU
- Kontroler sieci bezprzewodowej oraz oprogramowanie zarządzające dla kontrolera sieci Extreme Networks SUMMIT WM3400 WLAN CONTROLLER, Oprogramowanie Extreme Networks Ridgeline.

ZAMAWIAJĄCY **WYKONAWCA**