Moszczenica: Dostawa wielozadaniowego systemu zabezpieczeń sieciowych wraz z wdrożeniem i wsparciem technicznym w ramach realizacji projektu E-Leader szansą na przeciwdziałanie wykluczeniu cyfrowemu dla mieszkańców gmin: Moszczenica, Ujazd, Będków i Czarnocin.

Numer ogłoszenia: 108024 - 2014; data zamieszczenia: 31.03.2014

OGŁOSZENIE O ZAMÓWIENIU - dostawy

Zamieszczanie ogłoszenia: obowiązkowe.
Ogłoszenie dotyczy: zamówienia publicznego.

SEKCJA I: ZAMAWIAJĄCY

I. 1) **NAZWA I ADRES:** Gmina Moszczenica , ul. Kosowska 1, 97-310 Moszczenica, woj. łódzkie, tel. 044 6169570, faks 044 6169625.

Adres strony internetowej zamawiającego: www.moszczenica.pl

I. 2) **RODZAJ ZAMAWIAJĄCEGO:** Administracja samorządowa.

SEKCJA II: PRZEDMIOT ZAMÓWIENIA

II.1) OKREŚLENIE PRZEDMIOTU ZAMÓWIENIA

II.1.1) Nazwa nadana zamówieniu przez zamawiającego: Dostawa wielozadaniowego systemu zabezpieczeń sieciowych wraz z wdrożeniem i wsparciem technicznym w ramach realizacji projektu E-Leader szansą na przeciwdziałanie wykluczeniu cyfrowemu dla mieszkańców gmin: Moszczenica, Ujazd, Będków i Czarnocin..

II.1.2) Rodzaj zamówienia: dostawy.

II.1.4) Określenie przedmiotu oraz wielkości lub zakresu zamówienia: Przedmiotem zamówienia jest dostawa Wielozadaniowego systemu zabezpieczeń sieciowych wraz z wdrożeniem, przeszkoleniem pracowników i wsparciem technicznym w ramach realizowanego projektu: E-Leader szansą na przeciwdziałanie wykluczeniu cyfrowemu dla mieszkańców gmin: Moszczenica, Ujazd, Będków i Czarnocin. 1. Wsparcie techniczne. W ramach realizacji zamówienia muszą zostać dostarczone DWA kompletne, gotowe do pracy urządzenia pracujące, jako klaster (2 oddzielne lokalizacje sieciowe). Wraz z produktami wymagane jest dostarczenie opieki technicznej ważnej przez okres 5 lat od dnia podpisania bezusterkowego Protokołu Odbioru Dostawy. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Wsparcie techniczne świadczone będzie w języku polskim. Po dostarczeniu urządzeń Wykonawca przeprowadzi szkolenie/szkolenia pracowników Zamawiającego w wymiarze co najmniej 20 godzin, m.in. w zakresie uruchamiania i eksploatacji sprzętu, urządzeń, oprogramowania. Szkolenie/szkolenia odbędzie się w dniu uzgodnionym pomiędzy Zamawiającym, a Wykonawcą nie później jednak niż w ciągu 30 dni od daty podpisania bezusterkowego Protokołu Odbioru Dostawy. 2. Wsparcie konsultacyjne: Wymaga się, aby Wykonawca wraz z dostawą sprzętu i oprogramowania zapewnił bezpłatne wsparcie konsultacyjne w wymiarze nie większym niż 200 godzin w okresie 3 tygodni. Specjaliści wydelegowani do udzielenia wsparcia konsultacyjnego po otrzymaniu zgłoszenia od Zamawiającego muszą być dostępni w siedzibie

Zamawiającego nie później niż 5 godzin od momentu zgłoszenia. Wsparcie konsultacyjne musi być dostępne codziennie, 24 godziny na dobę, 7 dni w tygodniu. Wsparcie dotyczyć będzie uruchomienia i konfiguracji dostarczonego rozwiązania- klastra zabezpieczeń sieciowych w tym jego integracji z istniejącą i budowaną infrastrukturą E-Leader (w tym m. in. integracja z usługami AD, bezpieczne publikowanie usług z sieci LAN do sieci Internet, logowanie zdarzeń, URL Filtering. zabezpieczenia ruchu do/z Internetu bezpiecznego, bezpieczny dostęp do infrastruktury E-leader z Internetu, kontrola ruchu pomiędzy lokalizacjami, kontrola ruchu pomiędzy zasobami gminy i dmz oraz siecią użytkowników socjalnych i Ostatecznych Beneficjentów programu E-Leader.) Konfiguracja urządzeń musi zostać przeprowadzona przy współpracy z obecnym Wykonawcą sieci E-Leader oraz przy udziale pracowników Politechniki Częstochowskiej- autorów dokumentacji technicznej Projektu E-Leader szansą na przeciwdziałanie wykluczeniu cyfrowemu dla mieszkańców gmin: Moszczenica, Ujazd, Będków i Czarnocin. W kwestiach spornych decydujące zdanie należy do pracowników Politechniki Częstochowskiej. 3. Porty do przełączników (Cisco Catalyst 3750X - Przełączniki te wraz ze Wsparciem technicznym są w posiadaniu Zamawiającego). Wykonawca zobowiązany jest dostarczyć 20 autoryzowanych przez producenta wkładek typu 1000base-SX w pełni kompatybilnych z urządzeniami serii Cisco Catalyst 3750X. Dopuszcza się rozwiązanie równoważne pod warunkiem spełnienia poniższych minimalnych wymagań: 1) Muszą współpracować z urządzeniem posiadanym przez Zamawiającego 2) Musi być kompatybilny ze standardem 1000BASE -SX. 4. Klaster 2 urządzeń wchodzących w skład wielozadaniowego systemu zabezpieczeń sieciowych. Wymagania na pojedyncze urządzenie: 1) System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. 2) System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej. 3) Urządzenie zabezpieczeń musi posiadać przepływność w ruchu full-duplex nie mniej niż 2Gb/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 1Gb/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 250 000 jednoczesnych połączeń. 4) System zabezpieczeń musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. 5) Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność urządzenia zabezpieczeń przy włączonej identyfikacji aplikacji w ruchu full-duplex musi być nie mniejsza niż 2Gb/s. 6) Urządzenie zabezpieczeń musi być wyposażone w co najmniej 12 portów Ethernet 10/100/1000. Musi być możliwość zamontowania w urządzeniu minimum 8 interfejsów optycznych (SFP). 7) System zabezpieczeń musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych. Musi istnieć możliwość jednoczesnej konfiguracji i pracy poszczególnych interfejsów sieciowych w różnych trybach w pojedynczej instancji systemu zabezpieczeń. 8) Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN. 9) Urządzenie musi mieć możliwość pracy w trybie transparentnym L1 (bez konieczności nadawania adresu IP) oraz pozwalać na tworzenie transparentnych subinterfejsów, które będą obsługiwały ruch z wybranych vlanów lub podsieci IP. 10) Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jedna tabela routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i

OSPF. 11) Urządzenie musi obsługiwać nie mniej niż 6 wirtualnych systemów. Każdy z wirtualnych systemów musi tworzyć niezależny (wirtualny) firewall z własnymi regułami oraz musi mieć możliwość w pełni niezależnego zarządzania. 12) System zabezpieczeń musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji. 13) System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa. 14) Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). 15) System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona IntrusionPrevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. 16) System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona IntrusionPrevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. 17) System zabezpieczeń musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. 18) System zabezpieczeń musi identyfikować co najmniej 1700 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS, nie mniej niż: Skype, Gada-Gadu, Tor, BitTorrent, eMule. 19) System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa The Principle of LeastPrivilege, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. 20) Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama. 21) Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS. 22) Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM). 23) System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 24) System zabezpieczeń musi umożliwiać zarządzanie, kontrolę i wgląd w ruch nierozpoznany przez urządzenie. 25) System zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. 26) System zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. 27) System zabezpieczeń musi umożliwiać blokowanie transmisji plików, nie mniej niż:bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. 28) Urządzenie zabezpieczeń musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznego systemu typu Sand-Box plików wykonywalnych (exe, dll) przechodzących przez firewall z wydajnością modułu anty-wirus

czyli nie mniej niż1Gb/s w celu ochrony przed zagrożeniami typu zero-day. System zewnętrzny, na podstawie przeprowadzonej analizy, musi aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. 29) Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, oba), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu Sand-Box. 30) Administrator musi mieć możliwość dostępu do systemu analizy plików wykonywalnych w celu sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali. 31) System zabezpieczeń musi umożliwiać ochronę przed atakami typu Drive-by-download poprzez możliwość konfiguracji strony blokowania z dostępną akcją kontynuuj dla funkcji blokowania transmisji plików. 32) System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatycznyi posiadać nie mniej niż 20 milionów rekordów URL. 33) System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). 34) System zabezpieczeń musi posiadać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 35) System zabezpieczeń musi posiadać możliwość automatycznego pobierania listy stron WWW z zewnętrznego systemu w określonych przedziałach czasu i używania ich w politykach bezpieczeństwa. 36) System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. 37) System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). 38) System zabezpieczeń musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. 39) System zabezpieczeń musi posiadać możliwość uruchomienia modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). 40) System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 41) System zabezpieczeń musi posiadać możliwość uruchomienia modułu anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. 42) System zabezpieczeń musi posiadać możliwość uruchomienia modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). 43) System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 44) System zabezpieczeń musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. 45) System zabezpieczeń musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 46) System zabezpieczeń transparentnie ustala tożsamość użytkowników sieci (integracja z Active Directory, Citrix, LDAP i serwerami

Terminal Services). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników. 47) System zabezpieczeń musi umożliwiać integrację funkcjonalności mapowania nazw użytkowników do używanych adresów IP z rozwiązaniami niestandardowymi (np. kontrolerami sieci WiFi) za pomocą dostępnego interfejsu API. 48) Interfejs API musi być integralną częścią systemu zabezpieczeń umożliwiającą konfigurowanie i sprawdzanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). 49) Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. 50) Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. 51) System zabezpieczeń musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS i Kerberos. 52) System musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). 53) System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. 54) System zabezpieczeń zapewnia możliwość bezpiecznego zdalnego dostępu do chronionych zasobów w oparciu o standard SSL VPN bez konieczności stosowania dodatkowych licencji. 55) System zabezpieczeń musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci. 56) Urządzenie zabezpieczeń musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 100 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. 57) Nie jest dopuszczalne rozwiązanie, gdzie włączenie logowania na dysk może obniżyć wydajność urządzenia. 58) Urządzenie musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www. 59) Urządzenie musi mieć możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. 60) Urządzenie musi mieć możliwość stworzenia raportu o aktywności wybranego użytkownika na przestrzeni kilku ostatnich dni. 61) Urządzenie musi mieć możliwość generowania raportu na temat aktywności sieci typu Botnet wykrywanych przez system zabezpieczeń. 62) System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. 63) Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. IV. DODATKOWE INFORMACJE I WYMOGI ZAMAWIAJĄCEGO. 1. Wykonawca zobowiązuje się do udzielenia gwarancji na dostarczone sprzęt, urządzenia i oprogramowanie na okres minimum 60 miesięcy. Wymaga się aby udzielona gwarancja(e) była oparta o świadczenia gwarancyjne producenta (ów) skierowane do użytkowników z terenu Unii Europejskiej. 2. Termin gwarancji biegnie od dnia odbioru przez Zamawiającego sprzętu, urządzeń i oprogramowania stwierdzonego bezusterkowym

Protokołem Odbioru Dostawy. 3. Całość dostarczonego sprzętu, urządzeń i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na terenie Unii Europejskiej. 4. W przypadku powzięcia wątpliwości co do zgodności z umową, oferowanych sprzętu, urządzeń, oprogramowania Zamawiający jest uprawniony do: - zwrócenia się do ich producenta(ów) o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację) oraz - zlecenia ich producentowi(om) lub innym wskazanym przez producenta podmiotom i/lub inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych. Jeżeli inspekcja, o której mowa powyżej, wykaże niezgodność produktów z umową lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 30% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Zamawiającego w związku z inspekcją, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych. 5. Zamawiający wymaga by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy) na dzień poprzedzający dzień składania ofert. 6. Oferowane sprzęt, urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży. 7. Zamawiający wymaga aby dostarczone sprzęt, urządzenia i oprogramowanie były nowe (tj. nie używane i wyprodukowane nie wcześniej niż 6 miesięcy przed dniem dostawy do Zamawiającego. Zamawiający dopuszcza wcześniejsze (tj. przed dniem dostawy do Zamawiającego) rozpakowanie i uruchomienie sprzętu, urządzeń i oprogramowania wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania sprzętu, urządzeń i oprogramowania. Wykonawca jest obowiązany poinformować Zamawiającego o zamiarze rozpakowania sprzętu, urządzeń i oprogramowania jednakże nie zwalnia to Wykonawcy z obowiązku terminowej, zgodnej z niniejszą siwz dostawy. 8. Wykonawca oświadcza, iż korzystanie przez Zamawiającego z dostarczonego przez Wykonawcę sprzętu, urządzeń i oprogramowania nie będzie naruszało majątkowych praw autorskich osób trzecich. 9. W przypadku zgłoszenia przez Zamawiającego w okresie gwarancji wad, usterek lub awarii sprzętu, urządzeń lub oprogramowania Wykonawca zobowiązuje się do podjęcia czynności w ciągu 2 godzin od otrzymania zgłoszenia, przy czym w przypadku awarii obydwu urządzeń w miejsce jednego z nich musi zostać dostarczone urządzenie zastępcze o parametrach technicznych nie gorszych niż urządzenie zastępowane wraz z przeniesieniem konfiguracji otrzymanej od Zamawiającego w czasie nie dłuższym niż 6 godzin od momentu zgłoszenia. 10. W przypadku, gdy wykonawca nie wypełni warunków gwarancji lub nie zastosuje się do wymagań Zamawiającego określonych w niniejszej siwz Zamawiający jest uprawniony do usunięcia wad, usterek, awarii w drodze naprawy na ryzyko i koszt Wykonawcy zachowując przy tym uprawnienia wynikające z gwarancji przysługujące mu na podstawie umowy. W takich przypadkach Zamawiający ma prawo zaangażować wybrany przez siebie podmiot zewnętrzny do usunięcia wad, usterek, awarii, a Wykonawca zobowiązany jest pokryć związane z tym koszty w całości w ciągu 14 dni od daty otrzymania wezwania do zapłaty. 11. W przypadku, gdy naprawa sprzętu, urządzeń, oprogramowania potrwa dłużej niż 3 dni robocze Wykonawca na żądanie Zamawiającego dostarczy w przeciągu 3 dni roboczych zastępczy sprzęt, urządzenia, oprogramowanie o parametrach technicznych nie gorszych od sprzętu, urządzeń, oprogramowania naprawianych. 12. Wykonawca zobowiązuje się w czasie trwania gwarancji do nieodpłatnego dojazdu do Zamawiającego oraz nieodpłatnego usuwania zgłaszanych przez Zamawiającego wad, usterek, awarii. 13. W przypadku, gdy naprawa sprzętu, urządzeń, oprogramowania będzie wymagała dokonania naprawy poza siedzibą Zamawiającego, Wykonawca zobowiązuje się do nieodpłatnego transportu sprzętu, urządzeń, oprogramowania do miejsca naprawy i z miejsca naprawy do siedziby Zamawiającego. 14. Przy odbiorze sprzętu, urządzeń, oprogramowania na podstawie Protokołu Odbioru Dostawy Wykonawca zobowiązany jest dołączyć dokumenty gwarancyjne i instrukcje obsługi i eksploatacji. 15. W ramach niniejszego zamówienia do zadań oraz czynności Wykonawcy należeć będzie ponoszenie wobec Zamawiającego pełnej odpowiedzialności za realizację przedmiotu umowy, a także ponoszenie skutków

prawnych oraz finansowych za istotne zmiany wprowadzone z własnej inicjatywy w trakcie realizacji zamówienia bez akceptacji Zamawiającego i/lub z naruszeniem obowiązujących przepisów prawa oraz postanowień SIWZ. 16. Wykonawca zapewni nieograniczoną konsultację techniczną - telefoniczną i e-mailową w okresie gwarancji oraz bezpłatne wsparcie telefoniczne, za pośrednictwem poczty elektronicznej lub strony internetowej po upływie gwarancji co najmniej przez okres 5 lat..

II.1.6) Wspólny Słownik Zamówień (CPV): 32.42.00.00-3, 72.25.32.00-5.

II.1.7) Czy dopuszcza się złożenie oferty częściowej: nie.

II.1.8) Czy dopuszcza się złożenie oferty wariantowej: nie.

II.2) CZAS TRWANIA ZAMÓWIENIA LUB TERMIN WYKONANIA: Okres w dniach: 14.

SEKCJA III: INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM

III.1) WADIUM

Informacja na temat wadium: 1. Zamawiający żąda od wykonawcy wniesienia wadium w wysokości: 8 000 PLN. 2. Wadium wnosi się przed upływem terminu składania ofert. 3. Wadium może być wnoszone w jednej lub kilku następujących formach: 1) pieniądzu; 2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo - rozliczeniowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym; 3) gwarancjach bankowych; 4) gwarancjach ubezpieczeniowych; 5) poręczeniach udzielanych przez podmioty, o których mowa w art. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2007 r. Nr 42, poz. 275, z późn. zm.) 4. Wadium w formie pieniężnej należy wnieść na rachunek bankowy Zamawiającego w Banku: BS ZP o/ Moszczenica. Numer konta: 36 89730003 0070 0700 0707 0005 z adnotacją: Wadium - nr sprawy: INW.271. 9 .2014.D. Wadium musi być wniesione najpóźniej do upływu terminu składania ofert. 5. Poręczenia lub gwarancje bankowe, gwarancje ubezpieczeniowe, poręczenia udzielone przez podmioty, o których mowa w art. 6 ust.3 pkt.4 lit. b ustawy z dnia 9 listopada 2000r. o utworzeniu Polskiej agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2007 r. Nr 42, poz. 275, z 2008 r. Nr 116, poz. 730 i 732 i Nr 227, poz. 1505 oraz z 2010 r. Nr 96, poz. 620) do upływu terminu składania ofert powinny być złożone w kasie Urzędu Gminy. Uwaga: Nie należy załączać oryginału dokumentu wadialnego do oferty. Potwierdzona kserokopia dowodu wniesienia wadium powinna być załączona do oferty. Z chwilą zmiany terminu złożenia ofert przez Zamawiającego jednocześnie ulega zmianie termin (dzień) wniesienia wadium, godzina wniesienia pozostaje bez zmian chyba, że w zawiadomieniu o zmianie terminu złożenia ofert podano również zmienioną godzinę wniesienia wadium. 6. Z treści gwarancji (poręczenia) musi jednoznacznie wynikać jaki jest sposób reprezentacji Gwaranta. Gwarancja musi być podpisana przez upoważnionego (upełnomocnionego) przedstawiciela Gwaranta. Podpis winien być sporządzony w sposób umożliwiający jego identyfikację np. złożony wraz z imienną pieczątką lub czytelny (z podaniem imienia i nazwiska). Z treści gwarancji (poręczenia) winno wynikać bezwarunkowe, na każde żądanie zgłoszone przez Zamawiającego w terminie ważności gwarancji (poręczenia), zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 46 ust.4a i ust. 5 ustawy. 7. Oferta niezabezpieczona akceptowaną formą wadium, przez cały okres związania ofertą zostanie uznana za odrzuconą. 8. Za skuteczne wniesienie wadium w pieniądzu zamawiający uważa wadium, które w oznaczonym terminie znajdzie się na koncie zamawiającego. 9. Zamawiający zwraca wadium wszystkim wykonawcom niezwłocznie po wyborze oferty najkorzystniejszej lub unieważnieniu postępowania, z wyjątkiem wykonawcy, którego oferta została wybrana jako najkorzystniejsza, z zastrzeżeniem pkt. XIV. 10. Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, zamawiający zwraca wadium niezwłocznie po zawarciu umowy w sprawie zamówienia publicznego oraz wniesieniu zabezpieczenia należytego wykonania umowy, jeżeli jego wniesienia żądano, 11. Zamawiający zwraca niezwłocznie wadium, na wniosek wykonawcy, który wycofał ofertę przed upływem terminu składania ofert. 12. Zamawiający żąda

ponownego wniesienia wadium przez wykonawcę, któremu zwrócono wadium , jeżeli w wyniku rozstrzygnięcia odwołania jego oferta została wybrana jako najkorzystniejsza. Wykonawca wnosi wadium w terminie określonym przez zamawiającego; 13. Jeżeli wadium wniesiono w pieniądzu, zamawiający zwraca je wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wskazany przez wykonawcę. 14. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 ustawy, nie złożył dokumentów lub oświadczeń, o których mowa w art. 25 ust. 1 ustawy, lub pełnomocnictw, chyba że udowodni, że wynika to z przyczyn nieleżących po jego stronie. 15. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli wykonawca, którego oferta została wybrana: 1) odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie; 2) nie wniósł wymaganego zabezpieczenia należytego wykonania umowy; 3) zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie wykonawcy.

III.2) ZALICZKI

III.3) WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW

III. 3.1) Uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania

Opis sposobu dokonywania oceny spełniania tego warunku

Zamawiający nie precyzuje w tym zakresie wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny.

III.3.2) Wiedza i doświadczenie

Opis sposobu dokonywania oceny spełniania tego warunku

Ocena spełnienia warunków udziału w postępowaniu nastąpi na podstawie zasady spełnia/ nie spełnia, w oparciu o informacje zawarte w oświadczeniach i dokumentach żądanych na ich potwierdzenie przez Zamawiającego. Zamawiający uzna warunek za spełniony jeżeli Wykonawca Wykaże, iż w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał należycie co najmniej dwa zamówienia polegające na dostawie wielozadaniowego systemu zabezpieczeń sieciowych wraz z wdrożeniem. W przypadku wspólnego ubiegania się dwóch lub więcej Wykonawców o udzielenie niniejszego zamówienia, oceniane będą ich łączne kwalifikacje i doświadczenie.

III.3.3) Potencjał techniczny

Opis sposobu dokonywania oceny spełniania tego warunku

Zamawiający nie precyzuje w tym zakresie wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny. Zamawiający uzna ten warunek za spełniony jeżeli Wykonawca złoży stosowne oświadczenie.

III.3.4) Osoby zdolne do wykonania zamówienia

Opis sposobu dokonywania oceny spełniania tego warunku

Zamawiający nie precyzuje w tym zakresie wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny. Zamawiający uzna ten warunek za spełniony jeżeli Wykonawca złoży stosowne oświadczenie.

III.3.5) Sytuacja ekonomiczna i finansowa

Opis sposobu dokonywania oceny spełniania tego warunku

Ocena spełnienia warunków udziału w postępowaniu nastąpi na podstawie zasady spełnia/ nie spełnia, w oparciu o informacje zawarte w oświadczeniach i dokumentach żądanych na ich potwierdzenie przez Zamawiającego. Zamawiający uzna za spełniony jeżeli Wykonawca Jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na kwotę co najmniej 400.000,00 zł. W odniesieniu do warunku

opisanego w pkt. Ad. 4) SIWZ, w przypadku, gdy Wykonawca poda wartości w innych walutach niż PLN, Zamawiający dla oceny spełnienia warunku udziału w postępowaniu przyjmie średni kurs NBP (tabela A) dla kwoty ubezpieczenia od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem Zamówienia - na dzień wystawienia dokumentu, W przypadku wspólnego ubiegania się dwóch lub więcej Wykonawców o udzielenie niniejszego zamówienia, oceniana będzie ich łączna sytuacja ekonomiczna i finansowa - w tym celu dokumenty ma obowiązek złożyć ten lub Ci z Wykonawców, którzy w imieniu wszystkich wykazywać będą spełnianie tego warunku.

III.4) INFORMACJA O OŚWIADCZENIACH LUB DOKUMENTACH, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ NIEPODLEGANIA WYKLUCZENIU NA PODSTAWIE ART. 24 UST. 1 USTAWY

III.4.1) W zakresie wykazania spełniania przez wykonawcę warunków, o których mowa w art. 22 ust. 1 ustawy, oprócz oświadczenia o spełnianiu warunków udziału w postępowaniu należy przedłożyć:

- wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, głównych dostaw lub usług, w okresie ostatnich trzech lat przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy lub usługi zostały wykonane, oraz załączeniem dowodów, czy zostały wykonane lub są wykonywane należycie;

- określenie dostaw lub usług, których dotyczy obowiązek wskazania przez wykonawcę w wykazie lub złożenia poświadczeń, w tym informacja o dostawach lub usługach niewykonanych lub wykonanych nienależycie
  Zamawiający określa, iż dostawy, których dotyczy obowiązek wskazania przez Wykonawcę w wykazie obejmuje tylko dostawy potwierdzające spełnienie warunku wiedzy i doświadczenia określonego przez Zamawiającego w Rozdz. VIII ust.. 1 pkt 2 SIWZ;

- opłaconą polisę, a w przypadku jej braku, inny dokument potwierdzający, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia.

III.4.2) W zakresie potwierdzenia niepodlegania wykluczeniu na podstawie art. 24 ust. 1 ustawy, należy przedłożyć:

- oświadczenie o braku podstaw do wykluczenia;

- aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert;

- aktualne zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzające, że wykonawca nie zalega z opłacaniem podatków, lub zaświadczenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert;

- aktualne zaświadczenie właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy

Rolniczego Ubezpieczenia Społecznego potwierdzające, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia zdrowotne i społeczne, lub potwierdzenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert;

III.4.3) Dokumenty podmiotów zagranicznych
Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, przedkłada:
III.4.3.1) dokument wystawiony w kraju, w którym ma siedzibę lub miejsce zamieszkania potwierdzający, że:

- nie otwarto jego likwidacji ani nie ogłoszono upadłości - wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert;
- nie zalega z uiszczaniem podatków, opłat, składek na ubezpieczenie społeczne i zdrowotne albo że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia albo składania ofert;

III.4.4) Dokumenty dotyczące przynależności do tej samej grupy kapitałowej

- lista podmiotów należących do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów albo informacji o tym, że nie należy do grupy kapitałowej;

III.5) INFORMACJA O DOKUMENTACH POTWIERDZAJĄCYCH, ŻE OFEROWANE DOSTAWY, USŁUGI LUB ROBOTY BUDOWLANE ODPOWIADAJĄ OKREŚLONYM WYMAGANIOM
W zakresie potwierdzenia, że oferowane roboty budowlane, dostawy lub usługi odpowiadają określonym wymaganiom należy przedłożyć:

- inne dokumenty
  opis oferowanego urządzenia sporządzony wg wzoru stanowiącego Załącznik nr 6 do SIWZ

III.6) INNE DOKUMENTY
Inne dokumenty niewymienione w pkt III.4) albo w pkt III.5)
Formularz ofertowy - wg. Załącznika nr 1 do SIWZ, Kopia dowodu wniesienia wadium, Pełnomocnictwo (o ile w imieniu wykonawcy działa pełnomocnik).

SEKCJA IV: PROCEDURA

IV.1) TRYB UDZIELENIA ZAMÓWIENIA
IV.1.1) Tryb udzielenia zamówienia: przetarg nieograniczony.
IV.2) KRYTERIA OCENY OFERT
IV.2.1) Kryteria oceny ofert: najniższa cena.
IV.3) ZMIANA UMOWY

przewiduje się istotne zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy:

Dopuszczalne zmiany postanowień umowy oraz określenie warunków zmian

Zgodnie z art. 144 ustawy Zamawiający przewiduje zmiany zawartej umowy w przypadku m.in. zaistnienia następujących okoliczości: a) zmiany terminu wykonania zamówienia lub terminów płatności będących następstwem zaistnienia siły wyższej, okoliczności, których nie można było przewidzieć przy podpisywaniu Umowy lub zmiany harmonogramu spływu środków finansujących zamówienie z instytucji finansujących, b) zmiany powszechnie obowiązujących przepisów prawa, w zakresie mającym wpływ na realizację przedmiotu zamówienia, c) zmiany w przypadku rezygnacji z części zakresu zamówienia jeżeli będzie to niezbędne dla prawidłowej realizacji przedmiotu umowy d) zmiana terminu realizacji przedmiotu umowy spowodowana odmową wydania przez organy administracji lub inne podmioty wymaganych decyzji, zezwoleń, uzgodnień z przyczyn niezawinionych przez Wykonawcę, e) przedłużenie czasu trwania procedur administracyjnych, mających wpływ na termin wykonania przedmiotu zamówienia a nie wynikających z przyczyn leżących po stronie Wykonawcy, f) zmiana stawki podatku VAT w trakcie trwania umowy i wynikającej z tego tytułu zmiany wysokości wynagrodzenia określonego w § 14 ust. 1, g) gdy wykonanie zamówienia w określonym pierwotnie terminie nie leży w interesie Zamawiającego. h) zmiana dot. zaoferowanego przez Wykonawcę urządzenia oraz terminu realizacji umowy w przypadku zakończenia produkcji określonych produktów lub wycofanie ich z produkcji lub z obrotu na terytorium RP i) zmiana dot. zaoferowanego przez Wykonawcę urządzenia oraz terminu realizacji umowy w przypadku upadłości albo likwidacji producenta, dystrybutora lub gwaranta j) zmiana dot. zaoferowanego przez Wykonawcę urządzenia oraz terminu realizacji umowy w przypadku istotnych problemów finansowych, ekonomicznych lub organizacyjnych producenta, dystrybutora lub gwaranta uzasadniających ryzyko, że jego produkty, świadczenia itp. mogą nie zostać należycie wykonane lub nie będą miały odpowiedniej jakości albo wsparcia w przyszłości k) zmiana terminu realizacji przedmiotu umowy w przypadku uzasadnionych przyczyn technicznych lub funkcjonalnych powodujących konieczność zmiany sposobu wykonania umowy l) zmiana terminu realizacji przedmiotu umowy w przypadku konieczności zmiany terminu wykonania lub odbioru dostawy spowodowanej podjęciem przez Zamawiającego decyzji o przeprowadzeniu przez osobę trzecią kontroli jakości i sposobu prowadzenia dostawy.

IV.4) INFORMACJE ADMINISTRACYJNE

IV.4.1) Adres strony internetowej, na której jest dostępna specyfikacja istotnych warunków zamówienia: http://www.moszczenica.bipst.pl/index.php?grupa=511705

Specyfikację istotnych warunków zamówienia można uzyskać pod adresem: Urząd Gminy w Moszczenicy, ul. Kosowska 2, 97-310 Moszczenica, Referat Inwestycji i Rozwoju od poniedziałku do piątku, w godz. 8:00 - 15:00.

IV.4.4) Termin składania wniosków o dopuszczenie do udziału w postępowaniu lub ofert: 08.04.2014 godzina 10:00, miejsce: Urząd Gminy w Moszczenicy, ul. Kosowska 1, 97-310 Moszczenica w pok. nr 27.

IV.4.5) Termin związania ofertą: okres w dniach: 30 (od ostatecznego terminu składania ofert).

IV.4.16) Informacje dodatkowe, w tym dotyczące finansowania projektu/programu ze środków Unii Europejskiej: Zamówienie finansowane z Programu Operacyjnego Innowacyjna Gospodarka na lata 2007-2013. Termin realizacji zamówienia - 14 dni od daty podpisania umowy (nie później niż do dnia 05.05.2014 r.)..

IV.4.17) Czy przewiduje się unieważnienie postępowania o udzielenie zamówienia, w przypadku nieprzyznania środków pochodzących z budżetu Unii Europejskiej oraz niepodlegających zwrotowi środków z pomocy udzielonej przez państwa członkowskie Europejskiego Porozumienia o Wolnym Handlu (EFTA), które miały być przeznaczone na sfinansowanie całości lub części zamówienia: nie

WÓJT GMINY MOSZCZENICA
Marcin Piekarek