

Załącznik nr 7 do SIWZ

Wzór umowy

Umowa nr .....

Zawarta w Urzędzie Gminy w Moszczenicy w dniu ..... pomiędzy:

Gminą Moszczenica z siedzibą: 97 – 310 Moszczenica, ul. Kosowska 1
REGON: 590647948, NIP: 771 – 16 – 61- 550

reprezentowanym przez:
Pana Marcelego Piekarka – Wójta Gminy Moszczenica
Zwaną dalej **Zamawiającym**

działająca jako Lider Konsorcjum Gmin:
1) Moszczenica, ul. Kosowska 1, 97-310 Moszczenica
2) Ujazd, Pl. Kościuszki 6, 97-225 Ujazd,
3) Będków, ul. Parkowa 3, 97-319 Będków,
4) Czarnocin, ul. Główna 142, 97-318 Czarnocin

a ....., zwanym dalej Wykonawcą, reprezentowanym przez:
.....

Zamówienia udzielono w wyniku przeprowadzonego w trybie przetargu nieograniczonego postępowania o udzielenie zamówienia publicznego o wartości szacunkowej zamówienia przekraczającej kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2013 r. poz. 907).

§ 1
PRZEDMIOT UMOWY

Przedmiotem umowy 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".

Zamawiający zleca, a Wykonawca zobowiązuje się do:

1. Zrealizowania przedmiotu niniejszej umowy terminowo oraz z należytą starannością w pełnym zakresie rzeczowym opisanym w specyfikacji istotnych warunków zamówienia, zwanej dalej SIWZ i wskazanym w ofercie Wykonawcy;
3. Instalacji i uruchomienia;
4. Przeszkolenia pracowników Zamawiającego, m.in. w zakresie uruchamiania i eksploatacji sprzętu, urządzeń, oprogramowania. Szkolenie odbędzie się w dniu uzgodnionym pomiędzy Zamawiającym, a Wykonawcą nie później jednak niż w ciągu 30 dni od daty podpisania bezusterkowego Protokołu Odbioru Dostawy. Przeszkolenie pracowników Zamawiającego będzie podstawą do wystawienia Końcowego Protokołu Odbioru Przedmiotu Zamówienia;
5. Wykonywania obowiązków wynikających z udzielonej gwarancji zgodnie z SIWZ w zakresie usuwania wad, usterek, awarii sprzętu, urządzeń, oprogramowania.
6. Zapewnienia nieograniczonych konsultacji technicznych – drogą telefoniczną i e-mailową w okresie gwarancji oraz bezpłatne wsparcie telefoniczne, za pośrednictwem poczty elektronicznej lub strony internetowej po upływie gwarancji przez okres nie krótszy niż 5 lat.

§ 2
REALIZACJA UMOWY

1. Wykonawca oświadcza, że zapoznał się z treścią SIWZ w zakresie realizacji umowy i nie wnosi do niej uwag.
2. Wykonawca oświadcza, że dysponuje wystarczającymi środkami finansowymi, umiejętnościami, doświadczeniem i wiedzą oraz osobami zdolnymi do wykonania zamówienia, a także sprzętem i wyposażeniem niezbędnym dla prawidłowej realizacji przedmiotu umowy.
3. Wykonawca oświadcza, że znane mu są warunki związane z miejscem i sposobem realizacji przedmiotu umowy.



4. Przedmiot umowy, a także warunki gwarancji zostały określone w SIWZ.

§ 3

WYMAGANIA W ZAKRESIE URZĄDZENIA

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.

§ 4
SPOSÓB REALIZACJI UMOWY

1. Wykonawca zobowiązuje się wykonać przedmiot umowy zgodnie z zasadami współczesnej wiedzy technicznej, obowiązującymi przepisami, normami oraz wytycznymi zawartymi w SIWZ oraz ofertą Wykonawcy.
2. Zamawiający wymaga, aby wraz z dostawą Wykonawca dostarczył następujące dokumenty (sporządzone w języku polskim lub wraz z tłumaczeniem przysięgłym na język polski) :
   a) specyfikację funkcjonalną urządzenia,
   b) szczegółową instrukcję obsługi i eksploatacji,
   c) certyfikaty
   d) opis techniczny urządzenia,
   e) instrukcję lub procedury konserwacji,
   f) kartę gwarancyjną,
3. Wykonawca, w czasie dostawy urządzenia na trasie transportu winien zabezpieczyć przed zniszczeniem wszelkie ruchome i nieruchome mienie będące własnością Zamawiającego.
4. Wykonawca zobowiązany jest do przestrzegania przepisów bhp i ppoż podczas dostawy na trasie transportu i w pomieszczeniu wskazanym jako cel dostawy.
5. Wykonawca winien zorganizować i zrealizować przedmiot umowy w sposób umożliwiający ciągłość pracy Zamawiającego na trasie dostawy za wyjątkiem pomieszczenia – celu dostawy.

6. Wykonawca ma obowiązek uprzątnąć i zabrać ze sobą wszelkie opakowania zabezpieczające urządzenie w czasie transportu i na własny koszt zutylizować je zgodnie z obowiązującymi przepisami.
7. Wykonawca oświadcza, iż korzystanie przez Zamawiającego z dostarczonego przez Wykonawcę sprzętu, urządzeń i oprogramowania nie będzie naruszało majątkowych praw autorskich osób trzecich.
8. 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 wraz z przeniesieniem konfiguracji otrzymanej od Zamawiającego w czasie nie dłuższym niż 6 godzin od momentu zgłoszenia.
9. 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 lub 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.
10. W przypadku, gdy naprawa sprzętu, urządzeń lub 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.
11. Wykonawca zobowiązuje się w czasie trwania gwarancji do nieodpłatnego dojazdu do Zamawiającego oraz nieodpłatnego usuwania zgłaszanych przez Zamawiającego wad, usterek, awarii.
12. 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.

13. Przy odbiorze sprzętu, urządzeń, oprogramowania na podstawie Protokołu Odbioru Dostawy Wykonawca zobowiązany jest dołączyć dokumenty gwarancyjne i instrukcje obsługi i eksploatacji.
14. 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.
15. 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 przez okres nie krótszy niż 5 lat.

§ 5
DANE KONTAKTOWE STRON W CELU POROZUMIEWNIA SIĘ W TOKU REALIZACJI UMOWY

1. Wykonawca zobowiązuje się do wykonania dostawy, a Zamawiający do bieżącej kontroli i nadzoru właściwego wykonywania dostawy oraz do jego odbioru.
2. Do kontaktów i kontroli oraz nadzoru wynikających z realizacji niniejszej umowy wyznaczony został:
   - ze strony Zamawiającego: ....., tel. .....
   - ze strony Wykonawcy: ....., tel.....

§ 6
TERMIN DOSTAWY, OBOWIĄZKI WYKONAWCY I ODBIÓR PRZEDMIOTU UMOWY

1. Wykonawca zobowiązuje się do wykonania przedmiotu umowy w terminie ..... (14 dni od daty podpisania umowy, nie później niż do dnia 05.05.2014 r.)
2. W wyżej wymienionym terminie Wykonawca zobowiązuje się do dostarczenia sprzętu, urządzeń, oprogramowania własnym transportem, na własny koszt i na własne ryzyko oraz dokonania rozładunku i uruchomienia własnymi zasobami ludzkimi i sprzętowymi w miejscu wskazanym przez Zamawiającego oraz przeszkolenia pracowników



Zamawiającego, m.in. w zakresie uruchamiania i eksploatacji sprzętu, urządzeń, oprogramowania. (Szkolenie odbędzie się w dniu uzgodnionym pomiędzy Zamawiającym, a Wykonawcą nie później jednak niż w ciągu 30 dni od daty podpisania bezusterkowego Protokołu Odbioru Dostawy).

3. Z czynności odbioru dostawy będzie sporządzony **Protokół Odbioru Dostawy** zawierający wszelkie ustalenia dokonane w toku odbioru dostawy.
4. Wykonawca zawiadomi Zamawiającego o planowanym terminie dostawy najpóźniej na 3 dni przed tym terminem kontaktując się telefonicznie z ..... nr tel. .....w celu omówienia warunków dostawy na terenie obiektu.
5. Za dzień zakończenia realizacji przedmiotu zamówienia uważa się dzień, w którym podpisany zostanie przez Zamawiającego **Końcowy Protokół Odbioru Przedmiotu Zamówienia**;
6. W przypadku stwierdzenia podczas odbioru, że dostarczone sprzęt, urządzenia, oprogramowanie posiada wady, w szczególności jest niekompletne lub posiada ślady zewnętrznego uszkodzenia, Zamawiający odmówi odbioru części lub całości przedmiotu umowy, sporządzając protokół zawierający przyczyny odmowy odbioru wraz ze wskazaniem terminu do usunięcia wad. Opóźnienie w usunięciu wad dłuższe niż 14 dni w stosunku do terminu wskazanego przez Zamawiającego będzie równoznaczne z niezrealizowaniem przedmiotu umowy.
7. Wykonawca nie może powierzyć wykonywania zobowiązań wynikających z niniejszej umowy osobie trzeciej bez zgody Zamawiającego wyrażonej na piśmie.
8. Wykonawca ponosi pełną odpowiedzialność za szkody spowodowane przez pracowników Wykonawcy oraz osoby, którymi Wykonawca się posłużył w trakcie realizacji niniejszej umowy.

§ 7
WYNAGRODZENIE UMOWNE

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za wykonanie przedmiotu umowy wynagrodzenie ryczałtowe określone w formularzu ofertowym w kwocie ..... zł (słownie zł ..... brutto).

2. Wynagrodzenie, o którym mowa w ust. 1 uwzględnia wszelkie koszty związane z realizacją przedmiotu niniejszej umowy.



§ 8
ZAPŁATA WYNAGRODZENIA

1. Zapłata wynagrodzenia odbędzie się na podstawie faktury, którą Wykonawca wystawi po podpisaniu przez Zamawiającego **Końcowego Protokołu Odbioru Przedmiotu Zamówienia**.
2. Termin zapłaty wynagrodzenia należnego Wykonawcy będzie wynosił do 30 dni licząc od daty dostarczenia Zamawiającemu prawidłowo wystawionej faktury.
3. Za datę wykonania zapłaty wynagrodzenia Strony przyjmują datę obciążenia rachunku Wykonawcy kwotą płatności.
4. W przypadku zwłoki w zapłacie faktury Wykonawca ma prawo żądać od Zamawiającego zapłaty odsetek w ustawowej wysokości.

§ 9
ODSTĄPIENIE OD UMOWY

1. Stronom przysługuje prawo odstąpienia od umowy w następujących sytuacjach:
   a) Zamawiającemu przysługuje prawo odstąpienia od umowy, gdy:
      - Wykonawca nie dostarczył przedmiotu dostawy zgodnie z SIWZ oraz w ofertą i w terminie określonym w § 6 ust.1,
      - zostanie ogłoszona upadłość, wszczęte postępowanie likwidacyjne lub nastąpi likwidacja Wykonawcy,
      - zostanie wydane postanowienie, o wszczęciu egzekucji z majątku Wykonawcy lub zabezpieczenia majątku Wykonawcy dostawy.
   b) Wykonawcy przysługuje prawo odstąpienia od umowy, jeżeli Zamawiający zawiadomi Wykonawcę, iż wobec zaistnienia uprzednio nieprzewidzianych okoliczności nie będzie mógł spełnić swoich zobowiązań umownych wobec Wykonawcy.

§ 10
GWARANCJA



1. Wykonawca udzieli **60-o miesięcznej** gwarancji na dostarczone urządzenie. Udzielona gwarancja będzie zgodna z wymaganiami zawartymi w SIWZ, termin gwarancji biegnie od dnia podpisania Protokołu Odbioru Dostawy.
2. Wykonawca zobowiązuje się przenieść na Zamawiającego własność sprzętu, urządzeń, oprogramowania oraz wszelkie uprawnienia z tytułu gwarancji udzielonych przez producenta urządzenia, wydając w tym celu Zamawiającemu właściwe dokumenty gwarancyjne, najpóźniej w chwili podpisania Protokołu Odbioru Dostawy.
3. W przypadku wystąpienia w okresie gwarancji wad, usterek, awarii urządzenia, Zamawiający zawiadamia Wykonawcę, o powstałych wadach, usterkach, awariach a Wykonawca zobowiązuję się w ciągu 48 godzin od zgłoszenia do podjęcia niezbędnych czynności.
4. W przypadku gdy wykonawca nie wypełni warunków gwarancji lub nie zastosuje się do powyższego punktu 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 ciągu 14 dni od daty otrzymania dowodu zapłaty
5. W przypadku, gdy naprawa urządzenia potrwa dłużej niż 14 dni roboczych Wykonawca na żądanie Zamawiającego dostarczy w przeciągu 3 dni roboczych zastępcze urządzenie o zbliżonych parametrach technicznych.
6. Wykonawca zobowiązuje się w czasie trwania gwarancji do nieodpłatnego dojazdu do Zamawiającego oraz nieodpłatnego usuwania wad, usterek, awarii.
7. W przypadku gdy naprawa przedmiotu umowy będzie wymagała dokonania naprawy poza siedzibą Zamawiającego, Wykonawca zobowiązuje się do nieodpłatnego zabezpieczenia oraz transportu przedmiotu umowy do miejsca naprawy oraz z miejsca naprawy do siedziby Zamawiającego.
8. Zamawiający może dochodzić roszczeń z tytułu gwarancji za wady także po upływie terminu gwarancji, jeżeli zgłosi wadę przed upływem tego terminu.

§ 11
KARY UMOWNE



Strony ustalają, że obowiązującą ich formą odszkodowania będą kary umowne z następujących tytułów:

1. Wykonawca może naliczyć Zamawiającemu karę umowną za odstąpienie od umowy z przyczyn niezależnych od Wykonawcy w wysokości 10% wynagrodzenia umownego za wykonanie dostawy, od której realizacji odstąpiono.
2. Zamawiający może naliczyć Wykonawcy kary umowne:
   a) za zwłokę w wykonaniu przedmiotu umowy w wysokości 0,2% z wynagrodzenia umownego za każdy dzień zwłoki,
   b) za zwłokę w usunięciu wad stwierdzonych przy odbiorze lub ujawnionych w okresie gwarancji w wysokości 0,2% wynagrodzenia umownego za każdy dzień zwłoki liczony od upływu terminu do usunięcia wad,
   c) z tytułu odstąpienia od umowy z przyczyn niezależnych od Zamawiającego leżących po stronie Wykonawcy w wysokości 10% wynagrodzenia umownego.
3. Jeżeli wysokość zastrzeżonych kar umownych nie pokrywa poniesionej szkody, strony mogą dochodzić odszkodowania uzupełniającego na zasadach ogólnych Kodeksu Cywilnego. Zapłata kar umownych o których mowa w ust. 2 pkt a) i b) nie zwalnia Wykonawcy z obowiązku wykonania przedmiotu niniejszej umowy.

§ 12
DOPUSZCZALNE ZMIANY UMOWY

1. Zakazuje się istotnych zmian postanowień umowy w stosunku do treści oferty na podstawie której dokonano wyboru wykonawcy, chyba że Zamawiający przewidział możliwość dokonania takiej zmiany w ogłoszeniu o zamówieniu lub SIWZ oraz określił warunki takiej zmiany.
2. Wszelkie zmiany i uzupełnienia niniejszej umowy mogą być dokonane wyłącznie w formie pisemnego aneksu, podpisanego przez obie strony, pod rygorem nieważności.
3. 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.

§ 13
PRAWA AUTORSKIE

1. W przypadku, gdy realizacja Umowy obejmuje prace lub usługi mające charakter utworów w



rozumieniu przepisów z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 200 r. Nr 90 poz. 631. z późn. zm), Wykonawca przenosi na Zamawiającego z dniem podpisania bezusterkowego Protokołu Odbioru Dostawy całość majątkowych praw autorskich do powstałych rezultatów oraz zależnych praw majątkowych autorskich- tak do całości, jak i części utworu, na następujących polach eksploatacyjnych:

a) w zakresie utrwalenia i zwielokrotnienia we wszystkich znanych na dzień zawarcia Umowy technikach utrwalenia i zwielokrotnienia,
b) wprowadzenie do pamięci komputera, sieci komputerowych,
c) wykorzystania we wszelkich czynnościach związanych z działalnością wykonywaną przez Zamawiającego (w tym w ramach dalszych procesów inwestycyjnych).

2. W przypadku, gdy realizacja Umowy obejmuje prace lub usługi mające charakter utworów w rozumieniu przepisów z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 200 r. Nr 90 poz. 631. z późn. zm) Wykonawca zobowiązany jest w umowach z podwykonawcami zapewnić przejście na Zamawiającego całości majątkowych praw autorskich w zakresie określonym powyżej do rezultatów, w tym ich elementów składowych – prac wykonawców przy pomocy których Wykonawca realizuje Przedmiot Umowy, na wszelkich polach eksploatacyjnych potrzebnych Zamawiającemu do korzystania z rezultatów tych prac. Wykonawca jest zobowiązany zapewnić, że przenoszone majątkowe prawa autorskie nie będą w chwili ich przejścia obciążone prawami na rzecz osób trzecich, a także że osoby uprawnione z tytułu osobistych praw autorskich nie będą wykonywać takich praw w stosunku do Zamawiającego.
3. Wykonawca wyraża nieodpłatnie zgodę na dokonanie zmian przez Zamawiającego w utworach wskazanym w ust. 1.
4. Wykonawca przyjmuje na siebie wyłączną odpowiedzialność za wszelkie roszczenia z tytułu praw autorskich, związanych z utworami wskazanymi w ust. 1.
5. Wykonawca oświadcza, iż przedmiot umowy, tj. utwory, o których mowa w ust. 1 umowy są wolne od wad prawnych. W razie skierowania przeciwko Zamawiającemu roszczeń przez osoby trzecie, w szczególności z tytułu naruszenia przysługujących im praw autorskich, w wyniku korzystania przez Zamawiającego z utworu, określonego w ust. 1 w zakresie ustalonym w ust. 1 niniejszego paragrafu Zamawiający zawiadomi niezwłocznie o tym fakcie Wykonawcę, który zobowiązuje się do pełnego zaspokojenia powyższych roszczeń osób trzecich w przypadku ich zasadności.



§ 14
OBOWIĄZUJĄCE PRZEPISY

W sprawach nie uregulowanych w umowie zastosowanie mają przepisy Kodeksu Cywilnego oraz ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity Dz. U. 2010 r., Nr 113, poz. 759 z późn. zm.).

§ 15
OBOWIĄZYWANIE UMOWY

1. Strony zobowiązują się interpretować postanowienia umowy w sposób zmierzający do zapewnienia partnerskiej współpracy między nimi.
2. Spory powstałe w związku z umową będą rozstrzygane przez Strony przede wszystkim na drodze polubownej. Przed wniesieniem powództwa, każda ze Stron obowiązana jest co najmniej wezwać listem poleconym drugą Stronę do próby ugodowej.
3. W przypadku nie osiągnięcia porozumienia na drodze polubownej, spory powstałe w związku z umową będą rozstrzygane wyłącznie przez sąd właściwy dla siedziby Zamawiającego.

§ 16
KLAUZULA POUFNOŚCI

1. Wykonawca zobowiązuje się do zachowania w tajemnicy wszelkich informacji dotyczących umowy, jakie powziął lub poweźmie w związku z jej zawarciem oraz realizacją, w szczególności zobowiązuje się do zachowania w tajemnicy wszelkich dokumentów, opracowań, materiałów i innych informacji wyrażonych pisemnie lub w jakiejkolwiek innej formie w tym także informacji przekazywanych lub udostępnianych w ramach bezpośrednich, roboczych kontaktów przedstawicieli Zamawiającego z Wykonawcą, dotyczących umowy. Strony umowy będą związane klauzulą poufności bezterminowo.
2. Materiały udostępnione Wykonawcy do wglądu zostaną wykorzystane w celu realizacji umowy. Wszelkie kopie tych materiałów muszą zostać zniszczone po wykonaniu umowy, a oryginały powinny zostać zwrócone Zamawiającemu niezwłocznie po ich wykorzystaniu.
3. Obowiązek poufności, wynikający z ust. 1, nie obejmuje informacji powszechnie znanych oraz informacji, których obowiązek ujawnienia wynika z obowiązujących przepisów prawa.

§ 17

ROZPOWSZECHNIANIE I PUBLIKOWANIE INFORMACJI

1. Informacje związane z realizacją niniejszej umowy oraz dotyczące przedmiotu niniejszej umowy mogą być rozpowszechniane i/lub publikowane przez Wykonawcę wyłączenie w uzgodnieniu z Zamawiającym.
2. W przypadku określonym w pkt 1 Wykonawca uzgodni z Sekcją Wizerunku Zamawiającego treść rozpowszechnianych i/lub publikowanych informacji.

§ 18

ZAKAZ CESJI WIERZYTELNOŚCI

Wykonawca nie może przenieść na osobę trzecią jakichkolwiek swoich wierzytelności wynikających z niniejszej umowy (*zakaz cesji*). Ewentualna cesja wierzytelności przez Wykonawcę jest dopuszczalna wyłącznie za zgodą Zamawiającego wyrażoną w formie pisemnej pod rygorem nieważności.

§ 19

POSTANOWIENIA KOŃCOWE

1. Umowa została sporządzona w 5 jednobrzmiących egzemplarzach, 4 egzemplarze dla Zamawiających i 1 egzemplarz dla Wykonawcy.
2. Wykaz załączników stanowiących integralną część niniejszej umowy:
    1. Oferta Wykonawcy,
    2. Specyfikacja istotnych warunków zamówienia.

Wykonawca: **Zamawiający:**