Warszawa, dnia 10 grudnia 2015 r.

GŁÓWNY INSPEKTORAT WETERYNARII

DYREKTOR GENERALNY

GIWo 2622 – 66/2015

Zaproszenie do złożenia oferty

Główny Inspektorat Weterynarii (GIW), będący jednostką sektora finansów publicznych zaprasza Państwa do złożenia oferty, której przedmiotem jest **zakup usługi systemu ochrony sieci LAN, dostawa punktów dostępowych WiFi oraz przedłużenie gwarancji na urządzenie Barracuda Spam firewall.**

Niniejsze postępowanie nie jest prowadzone na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2013 r. poz. 907 ze zm.).

I. OPIS PRZEDMIOTU ZAMÓWIENIA

Zakres przedmiotowy:

zakup usługi systemu ochrony sieci LAN, dostawa punktów dostępowych WiFi oraz przedłużenie gwarancji na urządzenie Barracuda Spam firewall, zgodnych z opisem zamieszczonym w załączniku nr 1 do „Zaproszenia do złożenia oferty".

II. KRYTERIUM WYBORU

Podstawą oceny ofert będzie:

1) całkowita cena brutto podana w tabeli nr 1 „Formularza ofertowego", stanowiącego załącznik nr 2 do „Zaproszenia do złożenia oferty", przy czym cena jednostkowa brutto za urządzenie (punkt dostępowy WiFi) nie może przekraczać kwoty 3.499,00 zł;

2) całkowita cena brutto podana w tabeli nr 2 „Formularza ofertowego", stanowiącego załącznik nr 2 do „Zaproszenia do złożenia oferty", przy czym cena jednostkowa brutto za element platformy sprzętowej sieci LAN nie może przekraczać kwoty 3.499,00 zł.

Oferty nie spełniające powyżej określonych warunków zostaną odrzucone.

III. DOKUMENTY WYMAGANE DO ZŁOŻENIA OFERTY

1. Prawidłowo wypełniony i podpisany przez osobę/osoby upoważnione „Formularz ofertowy", stanowiący załącznik nr 2 do „Zaproszenia do złożenia oferty".
2. Pełnomocnictwo, jeżeli oferta jest podpisana przez pełnomocnika.

IV. OGÓLNE WARUNKI UMOWY

„Ogólne warunki umowy" stanowią załącznik nr 3 do „Zaproszenia do złożenia oferty".

V. SPOSÓB SKŁADANIA OFERTY

Ofertę należy przesłać e-mailem na podany niżej adres kontaktowy lub faksem pod numer 22 623-14-08 lub za pośrednictwem poczty, albo złożyć w Biurze Podawczym Ministerstwa Rolnictwa i Rozwoju Wsi ul. Wspólna 30 w Warszawie, w nieprzekraczalnym terminie do dnia **14 grudnia 2015 r. do godz. 14^{00}**.
Osobą upoważnioną do kontaktowania się z Wykonawcami jest:

Sebastian Sporniak
Telefon kontaktowy – 22 623-13-26
E-mail kontaktowy: sebastian.sporniak@wetgiw.gov.pl

Sposób opisania koperty, w której składana jest oferta:

GŁÓWNY INSPEKTORAT WETERYNARII
ul. Wspólna 30
00 – 930 Warszawa

„zakup usługi systemu ochrony sieci LAN, dostawa punktów dostępowych WiFi oraz przedłużenie gwarancji na urządzenie Barracuda Spam firewall"

Na kopercie lub faksie musi być umieszczona pieczątka podmiotu składającego ofertę.

ZASTĘPUJĄCY
DYREKTORA GENERALNEGO
Jacek Bonuta
Dyrektor Biura Pasz, Farmacji i Utylizacji

Załącznik nr 1

Opis przedmiotu zamówienia

1. Wymagania odnośnie usługi systemu ochrony sieci LAN

Świadczona usługa systemu ochrony musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej.

Wykonawca zapewni wszystkie poniższe funkcjonalności:

1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję ochrony powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
5. System realizujący funkcję ochrony powinien dysponować minimum 20 portami Ethernet 10/100/1000 Base-TX.
6. Możliwość tworzenia minimum 254 interfejsów wirtualnych definiowanych jako VLAN-y w oparciu o standard 802.1Q.
7. W zakresie ochrony obsługa nie mniej niż 3 miliony jednoczesnych połączeń oraz 22 tys. nowych połączeń na sekundę.
8. Przepustowość ochrony: nie mniej niż 2,5 Gbps dla pakietów 1518 B.
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 450 Mbps.
10. System realizujący funkcję ochrony powinien być wyposażony w lokalny dysk o pojemności minimum 32GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku do poszczególnych lokalizacji musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.

11. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - kontrola dostępu - zapora ogniowa klasy Stateful Inspection,
    - ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS),
    - poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
    - ochrona przed atakami - Intrusion Prevention System [IPS],
    - kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM,
    - kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP),
    - kontrola pasma oraz ruchu [QoS, Traffic shaping],
    - kontrola aplikacji oraz rozpoznawanie ruchu P2P,
    - możliwość analizy ruchu szyfrowanego protokołem SSL,
    - ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji,
12. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min. 950 Mbps.
13. Wydajność całego systemu bezpieczeństwa przy skanowaniu w trybie proxy z włączoną funkcją: Antivirus min. 300 Mbps.
14. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site,
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
    - Praca w topologii Hub and Spoke oraz Mesh,
    - Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF,
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth,
15. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.

16. Możliwość budowy min. 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
17. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
18. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
19. Możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ.
20. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
21. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
22. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
23. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
24. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
25. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    - haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
    - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
    - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych,
    - rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.

26. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    - ICSA dla funkcjonalności SSL VPN, IPSec, IPS, Antywirus,
    - ICSA lub EAL4 dla funkcjonalności Firewall.
27. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
28. Serwisy i licencje.
    - Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 1 roku.
29. Gwarancja oraz wsparcie:
    - System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczypospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej,
    - System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym /w ciągu 8 godzin/. Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (wykonawca winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej), mających swoją siedzibę na terenie Rzeczypospolitej Polskiej. Zgłoszenia serwisowe przyjmowane w trybie od poniedziałku do piątku poprzez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię 24x7 (należy podać numer infolinii).
30. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Rzeczypospolitej Polskiej, iż wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

2. Wymagania dotyczące punktu dostępowego WiFi

Tryb pracy	Urządzenie musi być tzw. „cienkim" punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. W celu zapewnienia spójności zarządzania i uzyskania wymaganego poziomu bezpieczeństwa, kontroler sieci bezprzewodowych ma być uruchomiony w obrębie zaproponowanego powyżej systemu ochrony sieci LAN oraz musi z nim współpracować.
Obudowa	Kompaktowa obudowa z tworzywa sztucznego umożliwiająca montaż na suficie wewnątrz budynku.
Moduł radiowy	Musi być wyposażone w dwa niezależne moduły radiowe pracujące odpowiednio w pasmach: 2.4 GHz b/g/n or 5 GHz a/n oraz 5 GHz a/n/ac. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID. Wymagana moc nadawania minimum 17dBm
Anteny	Minimum 4 anteny zewnętrzne (złącza RP-SMA)
Interfejsy	Minimum 1 interfejs w standardzie 10/100/1000 Base-TX
Zasilanie	Możliwość zasilania w standardzie PoE 802.3af

3. Przedłużenie gwarancji na urządzenie Barracuda Spam firewall

Przedłużenie gwarancji na funkcjonujące w Głównym Inspektoracie Weterynarii urządzenie Barracuda Spam firewall BSF 300 do wersji wirtualnej (Vx) dla systemów Vmware ESXi oraz ESX na okres 1 roku

Wdrożenie i instalacja:

Instalacja i konfiguracja usługi powinna być przeprowadzona przez uprawnionego inżyniera posiadającego aktualny certyfikat producenta. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Rzeczypospolitej Polskiej, iż posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

W zakresie świadczonej usługi, Wykonawca wykona:

- wdrożenie zaoferowane systemu zgodnie z zaleceniami zamawiającego dostosowując je do warunków pracy sieci informatycznej w Głównym Inspektoracie Weterynarii ,w szczególności:
  - przeniesie konfigurację z istniejącego urządzenia ochrony U150S do nowej usługi,
  - przekonfiguruje nowo zainstalowane rozwiązania w świetle obserwacji audytowych i oczekiwań funkcjonalnych Zamawiającego,
  - uruchomi i przekonfiguruje pracę punktów dostępowych do nowej usługi,
  - wykona testy zaimplementowanego rozwiązania pod kątem poprawności funkcjonowania nowej usługi w Głównym Inspektoracie Weterynarii,
- przeszkoli administratora sieci Głównego Inspektoratu Weterynarii, przeznaczając na to minimum 24h robocze.

Wszelkie prace związane z wdrażaniem oraz uruchamianiem powyższej usługi, wymagające jednocześnie czasowego zatrzymania usług takich jak dostęp do poczty, Internetu itp., powinny odbywać się poza godzinami pracy urzędu.

Załącznik nr 2

FORMULARZ OFERTOWY

Ja, niżej podpisany

.....

.....

działając w imieniu i na rzecz (nazwa i adres podmiotu składającego ofertę)

.....

.....

w odpowiedzi na zaproszenie do złożenia oferty nr GIWo 2622 - 66/2015, dotyczące:

zakupu usługi systemu ochrony sieci LAN, dostawa punktów dostępowych WiFi oraz przedłużenie gwarancji na urządzenie Barracuda Spam firewall.

składam niniejszą ofertę:

Tabela nr 1

Pozycja	**Liczba sztuk**	**Cena jednostkowa brutto (zł)**
Usługa Systemu ochrony sieci LAN	**1**	
Punkt dostępowy WiFi	**4**	
Przedłużenie gwarancji na urządzenie Barracuda Spam firewall (wersja Vx)	**1**	
Całkowita cena brutto:		**zł**

Tabela nr 2

Pozycja	**Liczba sztuk**	**Cena jednostkowa brutto (zł)**
Element platformy sprzętowej ochrony sieci LAN	**1**	
Całkowita cena brutto:		**zł**

Oświadczam, że zaoferowane na ww. urządzenia gwarancje (subskrypcje), są zgodne z opisem zamieszczonym w załączniku nr 1 do „Zaproszenia do złożenia oferty".

Uważam się za związanego niniejszą ofertą przez okres 30 dni od dnia upływu terminu składania ofert.

Załącznikami do niniejszego formularza oferty są:

1).....

2).....

....., dnia ..... 2015 r.

(miejscowość)

.....

(podpis upoważnionego przedstawiciela wraz z pieczątką imienną)

Załącznik nr 3

Ogólne warunki umowy:

Zakup usługi systemu ochrony sieci LAN, dostawa punktów dostępowych WiFi oraz przedłużenie gwarancji na urządzenie Barracuda Spam firewall:

1. Przedmiotem umowy jest zakup usługi systemu ochrony sieci LAN, dostawa punktów dostępowych WiFi oraz przedłużenie gwarancji na urządzenie Barracuda Spam firewall.
2. W ramach przedmiotu umowy, o którym mowa w ust. 1, Wykonawca w ciągu 5 dni kalendarzowych od dnia podpisania umowy:
   1) dostarczy Zamawiającemu licencje aktywacyjne oraz element platformy sprzętowej sieci LAN w ramach świadczenia usługi systemu ochrony sieci LAN w pomieszczeniach Głównego Inspektoratu Weterynarii, zlokalizowanego w Warszawie przy ulicy Wspólnej 30;
   2) dostarczy punkty dostępowe WiFi do pomieszczeń Głównego Inspektoratu Weterynarii, o których mowa w pkt 1;
   3) dokona przedłużenia gwarancji dla urządzenia Barracuda Spam firewall, na okres 1 roku;

   zgodnie z „Opisem przedmiotu zamówienia" znajdującym się w załączniku nr 1 do „Zaproszenia do złożenia oferty", stanowiącym załącznik do umowy.
3. W terminie, o których mowa w ust. 2, Wykonawca zobowiązuje się do realizacji przedmiotu umowy, w tym do wykonania prac instalacyjno-konfiguracyjnych, według specyfikacji technicznej, o której mowa w ust. 2, zgodnie z najwyższą starannością i na zasadzie zapewnienia najwyższej jakości wykonania, zgodnie z wolą Zamawiającego i zasadami współczesnej wiedzy technicznej. Wykonawca ponosi pełną odpowiedzialność za poprawność techniczną rozwiązań zastosowanych w ramach świadczonego zamówienia.
4. Wykonawca będzie wykonywać czynności, o których mowa w ust. 2 i 3, w dniach roboczych, w godzinach 8:15 – 16:15. Pod pojęciem dni roboczych należy rozumieć dni przypadające od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego. Czynności, które mogą spowodować przerwę w dostępie do usług sieciowych w Głównym Inspektoracie Weterynarii będą wykonywane poza ww. godzinami.
5. Zapłata wynagrodzenia nastąpi po wykonaniu przedmiotu umowy, o którym mowa w ust. 1, przelewem na rachunek Wykonawcy wskazany w fakturze, w terminie 14 dni licząc od dnia pokwitowania jego odbioru i doręczenia Zamawiającemu prawidłowo wystawionej faktury VAT, z zastrzeżeniem ust. 6.
6. Za zakup elementu platformy sprzętowej sieci LAN dostarczonego w ramach świadczenia usługi systemu ochrony sieci LAN Zamawiający zapłaci przelewem na rachunek Wykonawcy wskazany w osobnej fakturze, w terminie 14 dni od dnia otrzymania faktury VAT przez Zamawiającego. Wykonawca dostarczy Zamawiającemu osobną fakturę najpóźniej na 14 dni przed dniem 31 grudnia 2016 r.
7. Wykonawca wkalkuluje koszty użytkowania elementu platformy sprzętowej sieci LAN przez Zamawiającego do momentu jego zakupu, o którym mowa w ust. 6, w koszt świadczenia usługi systemu ochrony sieci LAN.
8. Faktury VAT zostaną wystawione na Inspekcję Weterynaryjną Główny Inspektorat Weterynarii, ul. Wspólna 30, 00-930 Warszawa, nr NIP: 526-22-83-496.

9. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1 % kwoty brutto należności, którą Wykonawca otrzymałby tytułem wynagrodzenia za każdy dzień opóźnienia w przypadku niewykonania przedmiotu umowy zgodnie z ust. 2 i 3.
10. Umowa może zostać rozwiązana ze skutkiem natychmiastowym, jeśli Wykonawca będzie realizował przedmiot umowy z opóźnieniem, które przekroczy o 5 dni termin wskazany w ust. 2.
11. W przypadku opóźnienia w realizacji przedmiotu umowy, które przekroczy o 5 dni termin wskazany w ust. 2, Zamawiający, niezależnie od uprawnienia do rozwiązania umowy ze skutkiem natychmiastowym, nałoży na Wykonawcę karę w wysokości 10 % kwoty brutto należności, którą Wykonawca otrzymałby tytułem wynagrodzenia.
12. Wykonawca zapewnia, że dostarczone w ramach realizacji przedmiotu umowy urządzenia będą:
    1) wolne od wad materiałowych i wykonawstwa;
    2) wolne od wad prawnych tj. nieobciążone prawami i roszczeniami osób trzecich;
    3) posiadać właściwości zgodne z wymaganiami Polskich Norm.
13. Wykonawca udziela 12-miesięcznej gwarancji na dostarczone w ramach niniejszej umowy urządzenia oraz system ochrony sieci LAN.
14. W okresie gwarancji, o której mowa w ust. 13, Wykonawca udziela bezpłatnych konsultacji (wsparcie techniczne) w zakresie wykonanej usługi (Wykonawca wyznacza osobę odpowiedzialną za kontakt pod ustalonym z Zamawiającym numerem telefonu).
15. Wykonawca oświadcza, że gwarancja, o której mowa ust. 13, obejmuje prawo Zamawiającego do:
    1) bezpłatnej aktualizacji oprogramowania do najnowszej wersji;
    2) wymiany niesprawnie działającego urządzenia na takie samo, lub o takich samych parametrach w czasie 48 godzin od momentu powiadomienia Wykonawcy o wystąpieniu usterki uniemożliwiającej poprawną pracę.
16. Serwis gwarancyjny będzie świadczony w miejscu użytkowania urządzeń oraz systemu ochrony sieci LAN. Zgłoszenie urządzeń oraz systemu ochrony sieci LAN do napraw gwarancyjnych dokonywane będzie w formie pisemnej, faksem lub e-mailem. Za moment zgłoszenia będzie uznawana data wysłania pisma lub widniejąca w raporcie transmisji danych lub potwierdzeniu odczytania wiadomości e-mail. Za wykonanie naprawy urządzeń oraz systemu ochrony sieci LAN będzie uznawana data pokwitowania wykonanej naprawy.
17. Całkowity czas naprawy urządzeń oraz systemu ochrony sieci LAN nie może przekroczyć 14 (czternastu) dni roboczych. Termin wykonania naprawy urządzeń oraz systemu ochrony sieci LAN liczony jest od momentu zgłoszenia wady Wykonawcy przez Zamawiającego do momentu pokwitowania wykonanej naprawy.
18. Koszty konfiguracji dostarczanych urządzeń a także koszty przewozu, opakowania i ubezpieczenia na czas dostawy i dojazdu w ramach serwisu gwarancyjnego, ponosi w całości Wykonawca.
19. W przypadku opóźnienia w wykonaniu naprawy określonej w ust. 17, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 50 zł za każdy dzień opóźnienia.
20. Zamawiający dokona protokolarnego odbioru przedmiotu umowy.
21. Zamawiający może odmówić dokonania protokolarnego odbioru przedmiotu umowy, o którym mowa w ust. 1, w przypadku:
    1) braku zgodności z umową lub z „Zaproszeniem do złożenia oferty";
    2) gdy przedmiot umowy jest uszkodzony lub niekompletny;
    3) gdy przedmiot umowy nie działa lub działa nieprawidłowo;
    4) gdy Zamawiający stwierdzi inne wady.
22. Prawidłowo sporządzony i podpisany przez obydwie strony umowy protokół odbioru jest podstawą oceny terminowości wykonania przedmiotu umowy.