

I. ZAMAWIAJĄCY:

Samodzielny Publiczny Zakład Opieki Zdrowotnej
Szpital Specjalistyczny MSWiA w Otwocku
ul. Bolesława Prusa 1/3
05-400 Otwock

SP ZOZ zaprasza do złożenia oferty na: **„Dostawę systemu/oprogramowania zapewniającego ochronę antywirusową i antymalware’ową sieci komputerowej SP ZOZ Szpitala Specjalistycznego MSWiA w Otwocku”**.

II. PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zakupu jest system zapewniający ochronę antywirusową i antymalware’ową wykorzystujący zarówno oprogramowanie zainstalowane lokalnie na urządzeniu końcowym jak i zaawansowane algorytmy obliczeniowe z tzw. „chmury obliczeniowej” dodatkowo wzmacniające efektywność ochrony sieci.
2. **Cechy systemu:**
 - 2.1. wykrywanie wirusów, Trojanów, spyware’ów, ataków typu „phishing” i „zero-day”,
 - 2.2. skanowanie poczty e-mail i jej załączników,
 - 2.3. skanowanie spakowanych i skompresowanych plików, dysków sieciowych, urządzeń zewnętrznych,
 - 2.4. skanowanie szybkie, pełne całego dysku oraz na żądanie umożliwiające skanowanie wybranych elementów systemu,
 - 2.5. system nie powinien wymagać aktualizacji lokalnych baz danych sygnatur wirusowych i zapewniać jednocześnie ochronę offline poprzez możliwość definiowania białych/czarnych list aplikacji oraz dedykowanych polityk bezpieczeństwa, na czas gdy system jest offline, obejmujących skanowanie w oparciu o zaawansowane heurystyki, blokowanie portów lub/i urządzeń peryferyjnych podłączonych do stacji roboczej lub serwera,
 - 2.6. możliwość skanowania w oparciu o heurystyki, które powinny wykorzystywać do analizy co najmniej kryteria wieku analizowanych aplikacji, ich popularności oraz typu,
 - 2.7. ochrona lokalnych przeglądarek internetowych pod kątem obrony przed atakami typu screen grabbers/scrapers, man-in-the-middle/middle-attacks, keyloggers,
 - 2.8. wbudowany firewall uniemożliwiający potencjalnie niebezpiecznym aplikacjom wykonywanie nieautoryzowanych połączeń,
 - 2.9. wbudowany mechanizm księgowania operacji podejrzanych plików i automatycznego przywracania systemu operacyjnego, rejestru i stanu poszczególnych zainfekowanych plików

- do stanu sprzed infekcji w przypadku przeniknięcia do systemu niebezpiecznych wirusów lub spyware'ów,
- 2.10. wbudowane w agenta rozwiązanie umożliwiające bezpieczne przetestowanie potencjalnie niebezpiecznych plików dla zwiększenia bezpieczeństwa chronionych urządzeń,
 - 2.11. skanowanie tylko plików, które pojawiły się jako nowe lub zostały zmienione od czasu ostatniego skanowania, by przyspieszyć działanie systemu,
 - 2.12. analiza behawioralna w oparciu o sposób zachowania plików na stacji roboczej i możliwość śledzenia zachowania niezauważanych plików,
 - 2.13. ochrona na poziomie jądra systemu z możliwością blokowania dostępu do pamięci systemowej i rejestru przez niezauważane aplikacje,
 - 2.14. analiza stron www, przeglądarek i wyników ich wyszukiwania pod kątem wykrycia zagrożeń, zanim użytkownicy będą w stanie wejść na wyszukiwaną stronę a także możliwość zmiany klasyfikacji lokalnych stron www w przypadku błędnie przypisanej klasyfikacji,
 - 2.15. weryfikacja stron internetowych pod kątem legalności ich pochodzenia, źródeł adresów DNS i IP oraz możliwości ataków typu phishing i ostrzeżenie w przypadku prób dostępu przez strony www do danych osobistych/poufnych,
 - 2.16. możliwość instalacji jako system bazowy lub jako dodatkowy system bezpieczeństwa pracujący bezkonfliktowo wraz z innym systemem bezpieczeństwa dla urządzeń końcowych w celu maksymalizacji ochrony stacji roboczych i serwerów,
 - 2.17. możliwość zarządzania portami i urządzeniami takimi jak CD, DVD, USB,
 - 2.18. możliwość zarządzania stacjami roboczymi zdalnie w tym możliwość uruchomienia i wyłączenia zdalnie stacji roboczej, wywołania i egzekucji komend DOS i rejestru, uruchamiania zdalnie skryptów wsparcia, skanowania i zdalnego czyszczenia końcówek,
 - 2.19. wsparcie dla systemów Windows XP, Vista, 7, 8, 8.1, Windows Server 2003 Standard, Enterprise, 32 i 64bit, Windows Server 2008 R2 Foundation, Standard, Enterprise, Windows Small Business Server 2008, 2011 i 2012,
 - 2.20. wsparcie dla systemów wirtualnych VMware vSphere 4 (ESX/ESXi3.0, 3.5, 4.0, 4.1, plus Workstation 6.5, 7.0, Server 1.0, 2.0), Citrix XenDesktop 5 i XenServer 5.0, 5.5, 5.6, Microsoft Hyper-V Server 2008, 2008 R2.6, wsparcie dla 32 i 64 bitowych systemów operacyjnych,
 - 2.21. możliwość instalacji na urządzeniach mobilnych, tabletach i smartfonach oraz wsparcie dla systemów Android oraz Apple iOS,
 - 2.22. agent instalowany na stacji roboczej nie powinien być większy niż 1 MB,
 - 2.23. typowa instalacja agenta na urządzeniu końcowym nie powinna zajmować dłużej niż 60 sekund,
 - 2.24. zaplanowane skanowanie systemu nie powinno wykorzystywać więcej niż 15% wydajności procesora.
3. **Ilość stanowisk:** 60;
 4. **Czas ochrony:** 1 rok, 2 lata, 3 lata (wariantowanie ceny) – Zamawiający zastrzega sobie prawo

- wyboru jednego z wariantów;
5. Wykonawca przedłoży ofertę cenową z podziałem na trzy warianty, z czego Zamawiający wybierze jeden z dostępnych wariantów:
 - 5.1. Wariant I: czas ochrony 1 rok;
 - 5.2. Wariant II: czas ochrony 2 lata;
 - 5.3. Wariant III: czas ochrony 3 lata.

III. TERMIN WYKONANIA ZAMÓWIENIA: 14 dni od dnia podpisania umowy.

IV. ISTOTNE WARUNKI ZAMÓWIENIA:

1. Oferta powinna zostać sporządzona zgodnie ze wzorem **załącznika nr 1** – formularz oferty do niniejszego zapytania ofertowego oraz podpisana przez osobę/y uprawnioną/e do reprezentacji Wykonawcy/ów.
2. Jedynym kryterium oceny ofert będzie cena brutto za realizację przedmiotu zamówienia.
3. Cena określona w ofercie powinna obejmować wszystkie koszty niezbędne do prawidłowej realizacji przedmiotu zamówienia, w tym upusty i rabaty.
4. Każdy Wykonawca może złożyć tylko jedną ofertę.
5. Postępowanie jest prowadzone w języku polskim. Wszelkie dokumenty składane w trakcie postępowania sporządzone w języku obcym należy składać wraz z tłumaczeniem na język polski.
6. Dokumenty są składane w formie oryginału lub kopii poświadczonych za zgodność z oryginałem przez Wykonawcę.
7. Wszelkie miejsca w ofercie, w których Wykonawca naniósł poprawki lub zmiany wpisywanej przez siebie treści muszą być parafowane przez osobę uprawnioną do reprezentacji Wykonawcy.
8. Rozliczenie transakcji nastąpi przelewem na rachunek bankowy wskazany na fakturze lub rachunku w ciągu 30 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT lub rachunku przez Wykonawcę. Podstawą wystawienia faktury lub rachunku jest bezusterkowy protokół odbioru końcowego podpisany przez przedstawicieli Zamawiającego i Wykonawcę.
9. Wynagrodzenie należne Wykonawcy będzie wynagrodzeniem ryczałtowym.
10. Wykonawcy będą związani ofertą przez okres 30 dni roboczych. Bieg terminu związania ofertą rozpoczyna się z upływem terminu składania ofert. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzenia ich ponownej oceny.
11. Przed upływem terminu składania ofert, w szczególnie uzasadnionych przypadkach Zamawiający może zmodyfikować treść zapytania ofertowego. Dokonana modyfikacja zostanie niezwłocznie przekazana wszystkim Wykonawcom, którzy otrzymali zapytanie ofertowe.
12. Zamawiający może zamknąć postępowanie bez wybrania żadnej oferty oraz zastrzega sobie prawo do negocjacji z wybranym/wybranymi Wykonawcą/Wykonawcami (w szczególności

- w przypadku złożenia ofert o takiej samej cenie).
13. Oferty złożone po terminie nie będą rozpatrywane.
 14. Zamawiający może wezwać Wykonawcę do wyjaśnień lub uzupełnień złożonej oferty w zakresie dokumentów dotyczących przedmiotu zamówienia wszystkich Wykonawców lub jedynie Wykonawcę z najkorzystniejszą ofertą.
 15. Ofertę w postaci załącznika nr 1 do zapytania ofertowego (formularz oferty) należy złożyć do dnia **20 września 2017 r. do godz. 10:00** w formie elektronicznej na adres k.gasowska@zozmswia.pl lub faksem na nr 22 779 46 71.
 16. W celu wykazania spełnienia przez Wykonawcę warunków udziału w postępowaniu Zamawiający żąda załączenia do oferty:
 - 16.1 oświadczenie o spełnianiu warunków udziału w postępowaniu zgodnie ze wzorem stanowiącym **załącznik nr 2** do zapytania ofertowego,
 - 16.2. aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,
 17. Osobą uprawnioną do kontaktu z oferentami jest:
Karolina Gąsowska, tel. 22 779-46-71 wew. 53, e-mail: k.gasowska@zozmswia.pl

ZATWIERDZAM

**Dyrektor
SP ZOZ Szpitala Specjalistycznego
MSWiA w Otwocku
/-/ Dariusz Kołodziejczyk**

**/ niepotrzebne skreślić*

(pieczęć Wykonawcy)

Załącznik nr 1 do
Zapytania ofertowego

FORMULARZ OFERTOWY

W odpowiedzi na zaproszenie do złożenia oferty na zakup i dostawa systemu/oprogramowania zapewniającego ochronę antywirusową i antymalware'ową sieci komputerowej SP ZOZ Szpitala Specjalistycznego MSWiA w Otwocku składamy niniejszą ofertę oświadczając, że akceptujemy w całości wszystkie warunki zawarte w zapytaniu ofertowym.

Nazwa Wykonawcy:.....

Adres:

Tel/ Fax:

e-mail:

REGON: NIP:

WARIAT I: czas ochrony 1 rok (dla 60 stanowisk komputerowych)

Oferujemy/oferuję wykonanie ww. przedmiotu zamówienia zgodnie z warunkami zapytania ofertowego za kwotę: netto ...%
VAT, brutto

słownie (.....).

WARIAT II: czas ochrony 2 lata (dla 60 stanowisk komputerowych)

Oferujemy/oferuję wykonanie ww. przedmiotu zamówienia zgodnie z warunkami zapytania ofertowego za kwotę: netto ...%
VAT, brutto

słownie (.....).

WARIAT III: czas ochrony 3 lata (dla 60 stanowisk komputerowych)

Oferujemy/oferuję wykonanie ww. przedmiotu zamówienia zgodnie z warunkami zapytania ofertowego za kwotę: netto ...%
VAT, brutto

słownie (.....).¹

¹ Zamawiający zastrzega sobie prawo wyboru wariantu

Oświadczenia i informacje dla Wykonawcy:

1. W przypadku niezgodności ceny napisanej cyfrowo i ceny napisanej słownie rozstrzygająca będzie cena napisana słownie.
2. Formularz ofertowy musi być podpisany przez osobę lub osoby upoważnione do reprezentowania Wykonawcy.
3. Oświadczamy, że:
 - 1) powyższe ceny zawierają wszystkie koszty jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty;
 - 2) w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia;
 - 3) dysponuje/my* środkami finansowymi niezbędnymi do realizacji całego zamówienia;
 - 4) zdobyłem/liśmy* konieczne informacje do przygotowania oferty;
 - 5) zapoznałem(y)* się z treścią zapytania ofertowego, wzoru umowy i nie wnoszę/imy * do nich zastrzeżeń;
 - 6) zapoznaliśmy się z lokalnymi warunkami realizacji przedmiotu zamówienia oraz zdobyliśmy wszelkie informacje konieczne do właściwego przygotowania niniejszej oferty;
 - 7) oferujemy wykonanie w całości przedmiotu zamówienia w terminie 14 dni od dnia podpisania umowy.
 - 8) jeżeli nastąpią jakiegokolwiek znaczne zmiany przedstawione w naszych dokumentach załączonych do oferty, natychmiast powiadomimy o nich Zamawiającego;
 - 9) faktury VAT/rachunki* będą płatne w terminie 30 dni od daty wpływu prawidłowo wystawionej faktury VAT/rachunku* do siedziby Zamawiającego:
4. Integralną część oferty stanowią następujące dokumenty :
 - 1)
 - 2)
5. Ja niżej podpisany/a zam.
..... wyrażam zgodę na przetwarzanie moich danych osobowych w związku z wykonywanym zamówieniem publicznym zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922 z późn. zm.).**

.....

(miejscowość) (data)

.....

(podpis oraz pieczęć Wykonawcy)

**/ niepotrzebne skreślić*

***/ oświadczenie powinno zostać wypełnione w przypadku, gdy Wykonawcą jest osoba fizyczna*

(pieczęć Wykonawcy)

ZAMAWIAJĄCY:

*Samodzielny Publiczny Zakład Opieki Zdrowotnej
Szpital Specjalistyczny MSWiA w Otwocku*

Składając ofertę w postępowaniu na **zakup i dostawa systemu/oprogramowania zapewniającego ochronę antywirusową i antymalware'ową sieci komputerowej SP ZOZ Szpitala Specjalistycznego MSWiA w Otwocku** spełniamy warunki udziału w niniejszym postępowaniu o udzielenie zamówienia publicznego określone w zapytaniu ofertowym i

OŚWIADCZAM(Y)*, ŻE:

wskazany(i) powyżej Wykonawca(y) spełnia(ją) warunki udziału w postępowaniu, dotyczące:

1. kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów;
2. sytuacji ekonomicznej lub finansowej;
3. zdolności technicznej lub zawodowej.

.....

(miejscowość) (data)

.....

(podpis oraz pieczęć Wykonawcy)

*/ niepotrzebne należy skreślić

UMOWA nr/..... - PROJEKT

W dniu 2017 r. w Otwocku pomiędzy:

Samodzielnym Publicznym Zakładem Opieki Zdrowotnej Szpitalem Specjalistycznym MSWiA w Otwocku z siedzibą przy ul. Prusa 1/3, 05-400 Otwock, wpisanym do rejestru prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XXI Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr: 0000177289, NIP: 532-10-17-768, Regon: 010158710, zwanym dalej Zamawiającym, reprezentowanym przez:

mgr Dariusza Kołodziejczyka,

a

..... z siedzibą w przy ul. wpisaną do rejestru przedsiębiorców prowadzonego przez pod nr KRS, REGON....., NIP....., kapitał zakładowy..... zwaną dalej Wykonawcą, reprezentowaną przez:

Panią/Pana*

lub

Panią/Panemzam. nr dowodu osobistego prowadzącą/-ym działalność gospodarczą pod firmą z adresem głównego miejsca wykonywania działalności w przy ul. zarejestrowanym/-ą w systemie centralnej ewidencji i informacji o działalności gospodarczej prowadzonej w systemie elektronicznym przez ministra właściwego ds. gospodarki na stronie internetowej pod adresem: <http://prod.ceidg.gov.pl> stan na dzień REGON NIP*, zwaną/-ym dalej Wykonawcą

na podstawie art. 4 pkt 8 ustawy Prawo zamówień publicznych została zawarta umowa o następującej treści:

§ 1.

1. Przedmiotem zakupu jest system zapewniający ochronę antywirusową i antymalware'ową wykorzystujący zarówno oprogramowanie zainstalowane lokalnie na urządzeniu końcowym jak i zaawansowane algorytmy obliczeniowe z tzw. „chmury obliczeniowej” dodatkowo wzmacniające efektywność ochrony sieci.

2. Cechy systemu:

- 2.1. wykrywanie wirusów, Trojanów, spyware'ów, ataków typu „phishing” i „zero-day”;
- 2.2. skanowanie poczty e-mail i jej załączników;
- 2.3. skanowanie spakowanych i skompresowanych plików, dysków sieciowych, urządzeń zewnętrznych;
- 2.4. skanowanie szybkie, pełne całego dysku oraz na żądanie umożliwiające skanowanie wybranych elementów systemu;
- 2.5. system nie powinien wymagać aktualizacji lokalnych baz danych sygnatur wirusowych i zapewniać jednocześnie ochronę offline poprzez możliwość definiowania białych/czarnych list aplikacji oraz dedykowanych polityk bezpieczeństwa, na czas gdy system jest offline, obejmujących skanowanie w oparciu o zaawansowane heurystyki, blokowanie portów lub/i urządzeń peryferyjnych podłączonych do stacji roboczej lub serwera;
- 2.4. możliwość skanowania w oparciu o heurystyki, które powinny wykorzystywać do analizy co najmniej kryteria wieku analizowanych aplikacji, ich popularności oraz typu;
- 2.5. ochrona lokalnych przeglądarek internetowych pod kątem obrony przed atakami typu screen grabbers/scrapers, man-in-the-middle/middle-attacks, keyloggers;
- 2.6. wbudowany firewall uniemożliwiający potencjalnie niebezpiecznym aplikacjom wykonywanie nieautoryzowanych połączeń;
- 2.7. wbudowany mechanizm księgowania operacji podejrzanych plików i automatycznego przywracania systemu operacyjnego, rejestru i stanu poszczególnych zainfekowanych plików do stanu przed infekcją w przypadku przeniknięcia do systemu niebezpiecznych wirusów lub spyware'ów;
- 2.8. wbudowane w agenta rozwiązanie umożliwiające bezpieczne przetestowanie potencjalnie niebezpiecznych plików dla zwiększenia bezpieczeństwa chronionych urządzeń;
- 2.9. skanowanie tylko plików, które pojawiły się jako nowe lub zostały zmienione od czasu ostatniego skanowania, by przyspieszyć działanie systemu;
- 2.10. analiza behawioralna w oparciu o sposób zachowania plików na stacji roboczej i możliwość śledzenia zachowania niezauważanych plików;
- 2.11. ochrona na poziomie jądra systemu z możliwością blokowania dostępu do pamięci systemowej i rejestru przez niezauważane aplikacje;
- 2.12. analiza stron www, przeglądarek i wyników ich wyszukiwania pod kątem wykrycia zagrożeń, zanim użytkownicy będą w stanie wejść na wyszukiwaną stronę a także możliwość zmiany

- klasyfikacji lokalnych stron www w przypadku błędnie przypisanej klasyfikacji;
- 2.13. weryfikacja stron internetowych pod kątem legalności ich pochodzenia, źródeł adresów DNS i IP oraz możliwości ataków typu phishing i ostrzeżenie w przypadku prób dostępu przez strony www do danych osobistych/poufnych;
 - 2.14. możliwość instalacji jako system bazowy lub jako dodatkowy system bezpieczeństwa pracujący bezkonfliktowo wraz z innym systemem bezpieczeństwa dla urządzeń końcowych w celu maksymalizacji ochrony stacji roboczych i serwerów;
 - 2.15. możliwość zarządzania portami i urządzeniami takimi jak CD, DVD, USB;
 - 2.16. możliwość zarządzania stacjami roboczymi zdalnie w tym możliwość uruchomienia i wyłączenia zdalnie stacji roboczej, wywołania i egzekucji komend DOS i rejestru, uruchamiania zdalnie skryptów wsparcia, skanowania i zdalnego czyszczenia końcówek;
 - 2.17. wsparcie dla systemów Windows XP, Vista, 7, 8, 8.1, Windows Server 2003 Standard, Enterprise, 32 i 64bit, Windows Server 2008 R2 Foundation, Standard, Enterprise, Windows Small Business Server 2008, 2011 i 2012;
 - 2.18. wsparcie dla systemów wirtualnych VMware vSphere 4 (ESX/ESXi3.0, 3.5, 4.0, 4.1, plus Workstation 6.5, 7.0, Server 1.0, 2.0), Citrix XenDesktop 5 i XenServer 5.0, 5.5, 5.6, Microsoft Hyper-V Server 2008, 2008 R2.6, wsparcie dla 32 i 64 bitowych systemów operacyjnych;
 - 2.19. możliwość instalacji na urządzeniach mobilnych, tabletach i smartfonach oraz wsparcie dla systemów Android oraz Apple iOS;
 - 2.20. agent instalowany na stacji roboczej nie powinien być większy niż 1 MB;
 - 2.21. typowa instalacja agenta na urządzeniu końcowym nie powinna zajmować dłużej niż 60 sekund;
 - 2.22. zaplanowane skanowanie systemu nie powinno wykorzystywać więcej niż 15% wydajności procesora.

§ 2.

1. Wykonawca, w czasie realizacji umowy ma obowiązek dostarczyć niezbędne oprogramowanie, kompletne, nie zawierające śladów użytkownika.
2. Wykonawca ponosi odpowiedzialność za zniszczenia wynikłe z jego winy w trakcie dostawy zakupionego oprogramowania.
3. Wykonawca oświadcza, że posiada odpowiednie kwalifikacje do profesjonalnego wykonania umowy.
4. Wykonawca ponosi odpowiedzialność za wykonanie przedmiotu umowy przy zachowaniu należytej staranności.
5. Wykonawca nie może powierzyć wykonania prac wynikających z niniejszej umowy osobie trzeciej bez zgody Zamawiającego.
6. Wykonawca nie może bez zgody Zamawiającego przenieść na osobę trzecią wierzytelności z niniejszej umowy.

§ 3.

1. Za wykonanie umowy ustala się wynagrodzenie w kwocie zł (słownie: zł) brutto.
2. Osobą odpowiedzialną za realizację umowy ze strony Zamawiającego jest Kierownik Sekcji Administracyjno – Gospodarczej albo inna osoba wyznaczona na piśmie przez Dyrektora.

§ 4.

1. Należność będzie płatna przelewem na rachunek bankowy Wykonawcy....., po prawidłowym wykonaniu prac będących przedmiotem niniejszej umowy, w terminie 30 dni od daty otrzymania prawidłowo wystawionej faktury przez Zamawiającego. Podstawą do wystawienia faktury jest bezusterkowy protokół odbioru końcowego podpisany przez przedstawicieli Zamawiającego i Wykonawcę.
2. Za dzień zapłaty uznaje się dzień obciążenia rachunku bankowego Zamawiającego.

§ 5.

Niniejsza umowa zawarta zostaje na okres 14 dni od dnia podpisania umowy.

§ 6.

Na wykonany przedmiot umowy Wykonawca udziela gwarancji na okres 12/24/36² miesięcy licząc od daty podpisania bezusterkowego protokołu odbioru końcowego. W okresie gwarancji Wykonawca obowiązany jest do nieodpłatnego usuwania stwierdzonych wad.

§ 7.

1. Zamawiający może odstąpić od umowy, w trybie natychmiastowym, z winy Wykonawcy, jeżeli:
 - 1.1. Wykonawca bez uzasadnionej przyczyny nie rozpoczął dostawy i nie kontynuuje jej, pomimo dodatkowego wezwania przez Zamawiającego;

§ 8.

1. Strony dopuszczają możliwość nieistotnych zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, w formie aneksu z zachowaniem formy pisemnej pod rygorem nieważności takiej zmiany.
2. Uzupełnianie, zmiany lub rozwiązanie umowy dla swej ważności wymagają formy pisemnej, w postaci aneksu do umowy.

§ 9.

1. Zamawiający zastrzega zastosowanie kar umownych w następujących przypadkach:

² W zależności od złożonej oferty/ wybranego wariantu przez Zamawiającego

- 1.1. za opóźnienie z tytułu nieterminowego zakończenia dostawy w wysokości 1,0 % wynagrodzenia brutto, o którym mowa w § 3 ust. 1 umowy, za każdy dzień opóźnienia;
- 1.2. za opóźnienie w usunięciu wad stwierdzonych przy odbiorze w wysokości 1,0 % wynagrodzenie brutto, o którym mowa w § 3 ust. 1 umowy, za każdy dzień opóźnienia, licząc od dnia wyznaczonego na usunięcie wad;
- 1.3. za odstąpienie od umowy z winy Wykonawcy w wysokości 10,00 % wynagrodzenia, o którym mowa w § 3 ust. 1 umowy.
2. Zamawiający jest uprawniony do potrącenia kary umownej z wynagrodzenia przysługującego Wykonawcy, po wystąpieniu uchybień, bez wezwania Wykonawcy do zapłaty, na co Wykonawca wyraża zgodę.
3. W przypadkach, gdy kary umowne nie okrywają poniesionych strat, Zamawiający może dochodzić odszkodowania uzupełniającego na drodze sądowej.
4. Wykonawcy przysługują odsetki ustawowe za opóźnienie w przypadku nieterminowego regulowania należności przez Zamawiającego.

§ 10.

W sprawach nie uregulowanych niniejszą umową zastosowanie mają przepisy Kodeksu cywilnego.

§ 11.

Ewentualne spory między stronami umowy rozstrzygać będzie Sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.

§ 12.

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

ZAMAWIAJĄCY

WYKONAWCA