Umowa nr

zawarta w dniu _____ w Grzegorzewie pomiędzy:

Gminą Grzegorzew, Plac 1000 Lecia Państwa Polskiego 1, 62-640 Grzegorzew

NIP 6662004649, REGON 311019148

reprezentowaną przez

Bożenę Dominiak – Wójta Gminy Grzegorzew

zwaną dalej „Zamawiającym”,

a

_____

zwanym dalej „Wykonawcą”,

W wyniku dokonania przez Zamawiającego wyboru oferty Wykonawcy w trybie podstawowym, o którym mowa w art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 ze zm.) dalej zwaną ustawą Pzp została zawarta Umowa o następującej treści:

**Przedmiot umowy § 1**

1. Przedmiotem umowy jest dostawa i wdrożenie wielofunkcyjnej zapory sieciowej (UTM) oraz dostawa przełączników sieciowych

1. **UTM (Unified Threat Management) wraz z instalacją, konfiguracją i przeszkoleniem dla administratora**

| Cecha | Wymagania minimalne |
|---|---|
| **Ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System bezpieczeństwa powinien sprawnie obsłużyć połączenia minimum 30 klientów sieci LAN. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji |

| | |
|---|---|
| | instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dostarczony sprzęt musi być przez wykonawcę zainstalowany i odpowiednio skonfigurowany. Wykonawca zapewni przeszkolenie w zakresie obsługi urządzenia.<br>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.<br>W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.<br>System musi wspierać IPv4 oraz IPv6 w zakresie:<br>• Firewall.<br>• Ochrony w warstwie aplikacji.<br>• Protokołów routingu dynamicznego. |

| | |
|---|---|
| **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.<br>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.<br>3. Monitoring stanu realizowanych połączeń VPN. |
| **Interfejsy, Dysk, Zasilanie:** | 1. System realizujący funkcję Firewall musi dysponować minimum 4 portami Gigabit Ethernet RJ-45.<br>2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.<br>3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.<br>4. System musi być wyposażony w zasilanie AC. |
| **Parametry wydajnościowe:** | 1. W zakresie Firewall'a obsługa nie mniej niż 600 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.<br>2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.<br>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps.<br>4. Wydajność szyfrowania IPSec VPN nie mniej niż 4,4 Gbps.<br>5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,0 Gbps.<br>6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.<br>7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 310 Mbps. |
| **Funkcje Systemu Bezpieczeństwa** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one |

| | |
|---|---|
| | być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:<br>1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.<br>2. Kontrola Aplikacji.<br>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.<br>4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.<br>5. Ochrona przed atakami - Intrusion Prevention System.<br>6. Kontrola stron WWW.<br>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.<br>8. Zarządzanie pasmem (QoS, Traffic shaping).<br>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).<br>10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.<br>11. Analiza ruchu szyfrowanego protokołem SSL. |

| | |
|---|---|
| **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.<br>2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<br>• Translację jeden do jeden oraz jeden do wielu.<br>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.<br>3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.<br>4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.<br>• Amazon Web Services (AWS).<br>• Microsoft Azure<br>• Cisco ACI.<br>• Google Cloud Platform (GCP).<br>• OpenStack.<br>• VMware vCenter (ESXi). |

| | |
|---|---|
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:<br>• Wsparcie dla IKE v1 oraz v2.<br>• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).<br>• Obsługa protokołu Diffie-Hellman grup 19 i 20.<br>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.<br>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.<br>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.<br>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.<br>• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.<br>• Mechanizm „Split tunneling" dla połączeń Client-to-Site.<br>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:<br>• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.<br>• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.<br>• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:<br>• Routingu statycznego.<br>• Policy Based Routingu.<br>• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |

| | |
|---|---|
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).<br>2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.<br>3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).<br>4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.<br>5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.<br>2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.<br>3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.<br>7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |

| | |
|---|---|
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.<br>2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.<br>4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.<br>5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.<br>2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.<br>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.<br>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.<br>5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.<br>6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.<br>7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |

| | |
|---|---|
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<br>• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.<br>• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.<br>• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.<br>2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.<br>3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.<br>2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.<br>3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.<br>4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.<br>5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.<br>6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.<br>7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |

| | |
|---|---|
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.<br>2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.<br>3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.<br>4. Musi istnieć możliwość logowania do serwera SYSLOG. |
| **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:<br>• ICSA lub EAL4 dla funkcji Firewall. |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:<br>a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen |
| **Gwarancja** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. |

| | |
|---|---|
| **Wsparcie technicznie, aktualizacje** | Producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. W przypadku modelu subskrypcyjnego licencje muszą być na okres trwałości projektu oraz dodatkowo musi zostać dołączona kalkulacja cenowa przedłużenia licencji na okres kolejnych 24 miesięcy w rozbiciu na okresy roczne. |

## 2. Przełączniki (switch) (4szt).

| Typ parametru | Wymagania |
|---|---|
| **Obudowa** | Switch do montażu naściennego. |
| **Porty** | Minimum 8 portów 10/100/1000Mbps RJ45 |
| **Wydajność przełącznika** | Prędkość magistrali minimum 16 Gb/s<br>Przepustowość (pakiety 64 bajtów) minimum 11 mpps<br>Rozmiar tablicy adresów MAC minimum 4 tys. |
| **Funkcjonalność warstwy II** | Obsługa minimum 200 wirtualnych sieci<br>Wsparcie dla agregacji LACP (802.3ad)<br>Obsługa min 4 grup LACP i 8 portów fizycznych per grupa<br>Obsługa funkcjonalnościi Voice vlan<br>Obsługa Multicastów, w tym MLD snooping oraz IGMP Snooping.<br>Mirroring portów<br>Diagnostyka stanu kabli<br>Zapobieganie pętlom |
| **Funkcjonalność warstwy III** | Obsługa minimum 16 wpisów routingu statycznego IPv4<br>Obsługa dhcp relay |
| **Zgodność z protokołami** | 802.1AB LLDP<br>802.1D Bridging, Spanning Tree<br>802.1p Ethernet Priority (User Provisioning and Mapping)<br>802.1Q VLAN Tagging, Double VLAN Tagging, GVRP<br>802.1S Multiple Spanning Tree (MSTP)<br>802.1v Protocol-based VLANs<br>802.1W Rapid Spanning Tree (RSTP)<br>802.1X Network Access Control, Auto VLAN<br>802.2 Logical Link Control<br>802.3ab Gigabit Ethernet (1000BASE-T)<br>802.3ac Frame Extensions for VLAN Tagging<br>802.3ad Link Aggregation with LACP<br>802.3AX LAG Load Balancing<br>802.3az Energy Efficient Ethernet (EEE)<br>802.3x Flow Control |

| | |
|---|---|
| **Zarządzanie** | Switch zarządzany, dostęp poprzez web interface szyfrowany (https), ssh |
| **Gwarancja** | Urządzenie fabrycznie nowe z gwarancją producenta na okres minimum 36 miesięcy |

2. Na realizację przedmiotowego zamówienia Zamawiający otrzymał grant w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczącego realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00
3. Wykonawca zobowiązuje się wykonać przedmiot umowy w szczególności zgodnie:
   a. z opisem zawartym w specyfikacji warunków zamówienia dalej „SWZ",
   b. ze złożoną ofertą,
   c. z zasadami wiedzy technicznej i obowiązującymi przepisami.
4. Wykonawca zobowiązuje się wykonać przedmiot zamówienia ze szczególną starannością z uwzględnieniem obowiązujących przepisów prawa, standardów i reguł wykonywania prac objętych niniejszą umową, a także zasad etyki zawodowej.
5. Wykonawca oświadcza, że dostarczony przedmiot umowy jest fabrycznie nowy, nieużywany.

**Terminy § 2**

1. Wykonawca zobowiązuje się dostarczyć przedmiot zamówienia na własny koszt i ryzyko w terminie do 30.04.2022r.
2. Wykonawca zobowiązuje się dostarczyć przedmiot zamówienia do Urzędu Gminy Grzegorzew w terminie zgodnym z Załącznikiem nr 8 do SWZ - Harmonogram prac dla zadania, nie później niż 30.04.2022r.
3. Zamawiający nie dopuszcza dostaw sukcesywnych.

**Obowiązki Wykonawcy § 3**

1. Dostawy należy dokonać do siedziby Zamawiającego, tj.: do Urzędu Gminy Grzegorzew, Plac 1000lecia Państwa Polskiego 1 w dni powszednie od poniedziałku do piątku w godzinach od 9.00-15.00. Wykonawca zobowiązuje się powiadomić Zamawiającego o dostawie co najmniej 3 dni robocze przed planowanym jej terminem.
2. Dostarczony przedmiot zamówienia będzie oryginalnie opakowany (opakowania nie mogą być naruszone), opakowania opisane, co do ich zawartości.
3. Do dostarczonego przedmiotu zamówienia Wykonawca dołączy wymagane świadectwa dopuszczenia do obrotu, atesty i certyfikaty, licencje na zainstalowane oprogramowanie instrukcje obsługi i karty gwarancyjne.
4. Odbiór przedmiotu umowy zostanie potwierdzony przez strony protokołem, przy czym protokół ten powinien zawierać co najmniej: nazwę sprzętu (z wyszczególnionymi wszystkimi częściami składowymi), ilość sprzętu, nazwę producenta, typ, model, numer seryjny.

**Gwarancja § 4**

1. Wykonawca udziela na sprzęt stanowiący przedmiot dostawy **…… miesięcznej gwarancji**, licząc od daty odbioru. Gwarancja świadczona będzie na miejscu u klienta z czasem reakcji serwisu do dwóch dni roboczych od zgłoszenia i skutecznym czasem naprawy nie dłuższym niż 14 dni kalendarzowych od przyjęcia zgłoszenia, z opcją pozostawienia uszkodzonych nośników danych u Zamawiającego (Zamawiający nie ponosi żadnych kosztów wymiany uszkodzonych nośników danych).
2. Serwis będzie realizowany przez producenta w jego autoryzowanym kanale serwisowym lub przez Wykonawcę.
3. W przypadku awarii, która nie zostanie usunięta w terminie 20 dni kalendarzowych, Wykonawca zobowiązany będzie do wymiany sprzętu na fabrycznie nowe, o parametrach nie gorszych od sprzętu uszkodzonego. Wymiana sprzętu na fabrycznie nowy nastąpi najpóźniej w 25 dniu kalendarzowym od dnia zgłoszenia awarii.

4. Niniejsza umowa stanowi dokument gwarancyjny bez konieczności składania dodatkowego dokumentu na okoliczność gwarancji.
5. Wszelkie koszty związane z wykonywaniem obowiązków gwarancyjnych ponosi Wykonawca.
6. Wykonawca na skutek zgłoszenia wady przez Zamawiającego podejmie niezwłocznie działania w celu usunięcia wady.
7. Do napraw gwarancyjnych Wykonawca jest zobowiązany użyć fabrycznie nowych materiałów i urządzeń o parametrach nie gorszych niż uszkodzone.
8. Wykonawca nie może odmówić usunięcia wad ze względu na koszty z tym związane.
9. Roszczenia z tytułu gwarancji jakości przysługują także po terminach upływu okresów, o których mowa w ust. 1, jeżeli wady były zgłoszone przed upływem tych terminów. Bieg terminu gwarancji rozpoczyna się z chwilą podpisania przez Zamawiającego protokołu odbioru końcowego.
10. Jeżeli Wykonawca nie usunie wad w wyznaczonym terminie przez Zamawiającego, Zamawiający może zlecić usunięcie wad stronie trzeciej na koszt Wykonawcy.
11. Wykonawca zobowiązuje się do usuwania wad na własny koszt.
12. Jeżeli Wykonawca nie usunie wady w terminie, Zamawiający jest uprawniony bez utraty praw wynikających z gwarancji, do zlecenia wykonania usunięcia wady wybranemu przez siebie podmiotowi na koszt i ryzyko Wykonawcy. Wykonawca zobowiązany jest do zwrotu poniesionych kosztów usunięcia wady w terminie 14 dni od pisemnego wezwania do zapłaty przez Zamawiającego.
13. Usunięcie wady powinno być stwierdzone protokolarnie.
14. Termin gwarancji ulega przedłużeniu o czas usunięcia wady, jeżeli zawiadomienie o wystąpieniu wady nastąpiło jeszcze w czasie trwania gwarancji.
15. Udzielenie gwarancji jakości przez innych gwarantów na poszczególne materiały wchodzące w skład przedmiotu umowy nie ogranicza, ani nie wyłącza w jakimkolwiek zakresie gwarancji jakości udzielonej przez Wykonawcę.

**Wynagrodzenie i zapłata wynagrodzenia § 5**

1. Za wykonanie przedmiotu umowy, określonego w §1 niniejszej umowy, Strony ustalają wynagrodzenie ryczałtowe w wysokości …… zł (słownie: ……..). Wynagrodzenie obejmuje należny podatek VAT.
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszystkie koszty związane z wykonaniem przedmiotu umowy.
3. Wynagrodzenie płatne będzie przelewem na konto bankowe Wykonawcy w terminie 30 dni od daty doręczenia poprawnie wystawionej faktury VAT Zamawiającemu.
4. Podstawę wystawienia faktury VAT stanowi podpisany protokół odbioru.
5. Zapłata nastąpi na rachunek bankowy Wykonawcy.
6. Fakturę VAT, o której mowa w ust. 4 należy wystawić na: Gmina Grzegorzew, Plac 1000-lecia Państwa Polskiego 1, 62-640 Grzegorzew, NIP 666-20-04-649
7. Zamawiający nie wyraża zgody na cesję wierzytelności wynikających z realizacji umowy na rzecz osób trzecich.

**Kary umowne § 6**

1. Wykonawca zapłaci Zamawiającemu karę umowną:
   1) za zwłokę w wykonaniu przedmiotu umowy – w wysokości 200,00 zł za każdy dzień zwłoki, licząc od dnia upływu terminu określonego w § 2,
   2) za zwłokę w usunięciu wad stwierdzonych w okresie gwarancji– w wysokości 100,00 zł za każdy dzień zwłoki od dnia wyznaczonego na usunięcie wad,
   3) za odstąpienie Zamawiającego od umowy z przyczyn zależnych od Wykonawcy – w wysokości 10 % wynagrodzenia brutto, określonego w § 5 ust. 1.
2. Wykonawca karę umowną zobowiązany jest zapłacić Zamawiającemu na podstawie pisemnego wezwania do zapłaty i noty księgowej w terminie 10 dni od ich wystawienia.
3. Zamawiający zastrzega sobie prawo potrącenia kary umownej z wynagrodzenia przysługującego Wykonawcy na podstawie stosownego oświadczenia w przypadku jej niezapłacenia w terminie określonym w ust. 2.
4. Łączna maksymalna wysokość kar umownych nie może przekroczyć 30 % wynagrodzenia brutto określonego w § 5 ust. 1 niniejszej umowy.

**§ 7**

1. Do spraw związanych z realizacją przedmiotu zamówienia upoważnione są następujące osoby:

1) ze strony Wykonawcy: ……..

2) ze strony Zamawiającego: …….

2. Zmiana osób, o których mowa w ust. 1, następuje poprzez pisemne powiadomienie drugiej strony i nie stanowi zmiany treści umowy.

**Zmiany umowy § 8**

1. Wprowadzenie zmian treści umowy wymaga formy pisemnej pod rygorem nieważności. Zmiany te nie mogą naruszać postanowień art. 455 ustawy Prawo zamówień publicznych.
2. Zamawiający na mocy art. 455 ust. 1 pkt. 1 ustawy dopuszcza możliwość zmiany zawartej umowy, w zakresie:

1/ zmian regulacji prawnych obowiązujących w dniu podpisania umowy;

2/ przedłużenia terminu wykonania przedmiotu umowy na skutek zaistnienia okoliczności niezawinionych przez Wykonawcę, na wniosek Wykonawcy i za zgodą Zamawiającego;

3/ zmiany oferowanego produktu na inny o parametrach nie gorszych niż zaoferowane przez Wykonawcę w ofercie i spełniających wymagania zawarte w specyfikacji warunków zamówienia – w sytuacji, gdy Wykonawca wykaże, że zaproponowane przez niego w ofercie produkty nie są dostępne na rynku w wyniku zakończenia ich produkcji lub wycofania ze sprzedaży;

4/ w przypadkach określonych w art. 455 ustawy Prawo zamówień publicznych.

**Odstąpienie od umowy § 9**

1. Zamawiający może odstąpić od umowy w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu;

2. W przypadku, o którym mowa w ust. 1 Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.

**Postanowienia końcowe § 10**

1. Wszelkie oświadczenia, uzgodnienia, powiadomienia, żądania stron będą doręczane listem poleconym, kurierem lub osobiście na adresy podane niżej:
   1) dla Wykonawcy: ……..
   2) dla Zamawiającego: Urząd Gminy Grzegorzew, Plac 1000-lecia Państwa Polskiego 1, 62-640 Grzegorzew

z zastrzeżeniem możliwości ich doręczania także na adres e-mail Zamawiającego grzegw@grzegorzew.pl

na adres e-mail Wykonawcy …… faksu ……. ze skutkiem na dzień wysłania e-mail lub faksu do godziny $15^{00}$ w dniu roboczym i potwierdzona listem poleconym nadanym najpóźniej następnego dnia roboczego.

2. W przypadku zmiany adresu Strona jest zobowiązana w terminie 14 dni powiadomić pisemnie drugą Stronę o nowym adresie. Zawiadomienie staje się skuteczne następnego dnia po jego doręczeniu.
   W przypadku braku zawiadomienia korespondencja wysłana na poprzedni adres uznana jest za doręczoną.

**§ 11**

1. Sprawy sporne, dla których Strony umowy nie znajdą polubownego rozwiązania, będą rozstrzygane przez właściwy sąd dla miejsca wykonania przedmiotu umowy.
2. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy ustaw: ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 z późn. zm.) oraz Kodeksu cywilnego, o ile przepisy ustawy Prawo zamówień publicznych nie stanowią inaczej.
3. Umowę sporządzono w 3 jednakowych egzemplarzach 2 dla Zamawiającego i 1 dla Wykonawcy.

**§12**

Integralną część umowy stanowią załączniki:

1) specyfikacja warunków zamówienia;
2) oferta Wykonawcy
3) opis przedmiotu zamówienia
4) Załącznik nr 8 do SWZ - Harmonogram prac dla zadania

**ZAMAWIAJĄCY** **WYKONAWCA**