

(WZÓR) UMOWA
Wymiana kamer wraz z modernizacją systemu monitoringu

zawarta w dniu r. w Mławie pomiędzy:

Przedsiębiorstwem Energetyki Ciepłej w Mławie Spółka z ograniczoną odpowiedzialnością z siedzibą w Mławie, ul. Powstańców Styczniowych 3, 06-500 Mława, wpisanym do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000123088, NIP 5690002805, REGON 130344960, reprezentowanym przez:

1)

zwanym dalej „Zamawiającym”,

a

.....
z siedzibą
wpisanym do
NIP, REGON,
reprezentowanym przez:

1)

2)

zwanym dalej „Wykonawcą”.

§ 1. PRZEDMIOT UMOWY

1. Przedmiotem umowy jest wykonanie przez Wykonawcę na rzecz Zamawiającego zadania pn.: „Wymiana kamer wraz z modernizacją systemu monitoringu”, obejmującego w szczególności dostawę, montaż, konfigurację, uruchomienie i integrację elementów systemu monitoringu oraz zapewnienie ich bezpiecznej eksploatacji, zgodnie z opisem przedmiotu zamówienia stanowiącym Załącznik nr 7 do zapytania ofertowego, obowiązującymi przepisami prawa, w tym w zakresie ochrony danych osobowych i cyberbezpieczeństwa, a także zasadami wiedzy technicznej oraz zgodnie z zasadami przetwarzania danych osobowych określonymi w Załączniku do umowy – Umowie powierzenia przetwarzania danych osobowych i zobowiązaniu poufności.
2. Wykonawca zobowiązuje się do przetwarzania wyłącznie danych osobowych niezbędnych do realizacji przedmiotu umowy oraz zgodnie z zasadą minimalizacji danych wynikającą z RODO.
3. Zakres prac obejmuje w szczególności:
 - demontaż istniejących kamer,
 - montaż nowych kamer IP (zewnętrznych i wewnętrznych),
 - poprowadzenie okablowania do szafy RACK
 - instalację i konfigurację rejestratora, switcha PoE, monitora i UPS,
 - sporządzenie dokumentacji powykonawczej,

- inne prace niezbędne do prawidłowego i bezpiecznego działania systemu, w tym zapewnienie odpowiedniej konfiguracji pod kątem bezpieczeństwa teleinformatycznego, realizację szkoleń dla wskazanych osób Zamawiającego z zasad bezpiecznej obsługi systemu oraz opracowanie i przekazanie Zamawiającemu instrukcji eksploatacji z uwzględnieniem zasad bezpieczeństwa
 - 4. Wykonawca ponosi pełną odpowiedzialność za działania i zaniechania swoich podwykonawców jak za działania własne oraz zapewnia, że podwykonawcy spełniają wymagania w zakresie bezpieczeństwa i poufności określone w niniejszej umowie.
 - 5. Wykonawca zobowiązuje się do realizacji przedmiotu umowy zgodnie z wymaganiami:
 - ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
 - dyrektywy NIS2 w zakresie mającym zastosowanie do Zamawiającego,
 - norm ISO/IEC 27001 dotyczących bezpieczeństwa informacji,
 - norm ISO 50001 w zakresie zapewnienia ciągłości i bezpieczeństwa infrastruktury wspierającej procesy energetyczne,
 - polityk bezpieczeństwa i procedur obowiązujących u Zamawiającego.
 - 6. Wykonawca zobowiązuje się do przekazania Zamawiającemu pełnych praw administracyjnych do systemu, w tym:
 - loginów i haseł administratora,
 - kopii konfiguracji,
 - dokumentacji adresacji IP,
 - konfiguracji VLAN,
 - wykazu kont użytkowników,
 - informacji o aktywnych usługach zdalnego dostępu.
 - 7. Wykonawca zobowiązany jest do usunięcia własnych kont administracyjnych po odbiorze końcowym, chyba że Zamawiający postanowi inaczej.
 - 8. Wykonawca oświadcza, że dostarczone urządzenia i oprogramowanie:
 - nie posiadają statusu End of Life (EOL),
 - nie posiadają statusu End of Support (EOS),
- są objęte wsparciem producenta przez minimum miesięcy od dnia odbioru końcowego.

§ 2. TERMIN REALIZACJI

1. Wykonawca zobowiązuje się do wykonania przedmiotu umowy w terminie **60 dni od dnia podpisania umowy, tj. do dnia**
2. W przypadku przewidywanego opóźnienia w realizacji przedmiotu umowy Wykonawca jest zobowiązany niezwłocznie, nie później jednak niż w terminie 3 dni od powzięcia wiadomości o przyczynach opóźnienia, pisemnie poinformować Zamawiającego, wskazując przyczyny oraz propozycję działań naprawczych. Nie zwalnia to Wykonawcy z odpowiedzialności z tytułu kar umownych i odszkodowania uzupełniającego.
3. Zamawiający jest uprawniony do wstrzymania odbioru robót w przypadku stwierdzenia istotnych wad lub naruszeń wymagań bezpieczeństwa, w tym cyberbezpieczeństwa, do czasu ich usunięcia.
4. W przypadku wystąpienia incydentu bezpieczeństwa mogącego mieć wpływ na system monitoringu lub infrastrukturę Zamawiającego, Wykonawca zobowiązany jest:
 - niezwłocznie zabezpieczyć system,
 - współpracować z Zamawiającym przy analizie incydentu,
 - przekazać raport z incydentu,
 - wdrożyć działania naprawcze i zapobiegawcze.
5. W przypadku naruszenia ochrony danych osobowych Wykonawca zobowiązany jest do niezwłocznego poinformowania Zamawiającego, nie później niż w terminie 24 godzin od stwierdzenia naruszenia.
6. Zamawiającemu przysługuje prawo odstąpienia od umowy w całości lub w części, ze skutkiem natychmiastowym, w przypadku:

- 1) opóźnienia w wykonaniu przedmiotu umowy przekraczającego 7 dni;
 - 2) stwierdzenia istotnych naruszeń wymagań dotyczących bezpieczeństwa, w tym cyberbezpieczeństwa, które nie zostały usunięte w wyznaczonym przez Zamawiającego terminie;
 - 3) rażącego naruszenia obowiązków umownych przez Wykonawcę, w tym obowiązków w zakresie poufności lub ochrony danych osobowych;
 - 4) wszczęcia wobec Wykonawcy postępowania upadłościowego lub restrukturyzacyjnego, lub zaprzestania prowadzenia działalności.
7. W razie odstąpienia od umowy z przyczyn, o których mowa w ust. 6, Zamawiający zachowuje prawo do naliczenia kar umownych przewidzianych w § 5 oraz dochodzenia odszkodowania uzupełniającego.

§ 3. WYNAGRODZENIE

1. Wynagrodzenie za wykonanie przedmiotu umowy wynosi:
 - netto: Zł; (słownie:.....)
 - VAT (.....%): zł
 - brutto: zł (słownie:)
2. Wynagrodzenie ma charakter ryczałtowy i obejmuje wszelkie koszty związane z należytyym wykonaniem umowy, w tym koszty dojazdów, robocizny, materiałów, licencji, szkoleń, ubezpieczeń, utylizacji odpadów, spełnienia wymogów bezpieczeństwa i cyberbezpieczeństwa oraz przeniesienia praw określonych w niniejszej umowie.
3. Wynagrodzenie obejmuje również:
 - dostarczenie legalnych licencji,
 - aktualizacji bezpieczeństwa,
 - wsparcia producenta,
 - przekazania praw do korzystania z oprogramowania zgodnie z warunkami licencyjnymi producenta.
4. Wynagrodzenie obejmuje również wszelkie koszty związane z realizacją obowiązków wynikających z przepisów o ochronie danych osobowych oraz umowy powierzenia przetwarzania danych osobowych.
5. Wykonawca oświadcza, że wszelkie dostarczone urządzenia, firmware i oprogramowanie pochodzą z legalnego i autoryzowanego kanału dystrybucji.
6. Wynagrodzenie płatne będzie jednorazowo po należytyym wykonaniu całości przedmiotu umowy i podpisaniu przez Strony bezusterkowego protokołu odbioru końcowego, na podstawie prawidłowo wystawionej faktury VAT. Termin płatności wynosi 30 dni od dnia doręczenia Zamawiającemu faktury.
7. Zamawiający jest uprawniony do potrącenia z wynagrodzenia należnego Wykonawcy przysługujących mu kar umownych oraz innych wymagalnych należności wynikających z niniejszej umowy, bez potrzeby uzyskiwania odrębnej zgody Wykonawcy.
8. Jeżeli zgodnie z obowiązującymi przepisami prawa podatkowego Wykonawca jest zobowiązany do wystawiania faktur w postaci faktur ustrukturyzowanych przy użyciu Krajowego Systemu e-Faktur (KSeF) albo z niego dobrowolnie korzysta, Wykonawca wystawia faktury dokumentujące wynagrodzenie należne na podstawie niniejszej umowy wyłącznie jako faktury ustrukturyzowane w KSeF, na dane identyfikacyjne Zamawiającego oraz z użyciem identyfikatora KSeF Zamawiającego.
9. Strony zgodnie postanawiają, że w przypadku faktur ustrukturyzowanych wystawianych przy użyciu KSeF za dzień doręczenia faktury Zamawiającemu uważa się dzień nadania tej fakturze numeru identyfikującego w KSeF, pod warunkiem że faktura została prawidłowo wystawiona na dane Zamawiającego i jest widoczna na koncie Zamawiającego w KSeF. Termin płatności, o którym mowa w ust. 6, biegnie od dnia następującego po dniu doręczenia faktury w rozumieniu zdania poprzedzającego.

§ 4. GWARANCJA

1. Wykonawca udziela gwarancji na wykonane roboty oraz zamontowane urządzenia na okres nie krótszy niż miesięcy od daty odbioru końcowego." (lub inny minimalny okres, jaki Zamawiający uzna za właściwy).
2. W okresie gwarancji Wykonawca zapewni całodobową (24/7) możliwość zgłaszania awarii oraz usuwanie wad krytycznych uniemożliwiających korzystanie z systemu. Wykonawca zapewnia czas reakcji serwisowej nie dłuższy niż 48 godzin od zgłoszenia awarii, a dla awarii krytycznych uniemożliwiających korzystanie z systemu - podjęcie działań nie później niż następnego dnia roboczego.
3. Okres gwarancji ulega przedłużeniu o czas, w którym z powodu występowania wad przedmiot umowy nie mógł być używany zgodnie z przeznaczeniem.
4. W razie bezskutecznego upływu terminu na usunięcie wad Zamawiający może zlecić ich usunięcie osobie trzeciej na koszt i ryzyko Wykonawcy, bez utraty uprawnień z tytułu gwarancji i rękojmi.
5. W okresie gwarancji Wykonawca zobowiązany jest do instalowania krytycznych aktualizacji bezpieczeństwa nie później niż w terminie 14 dni od ich publikacji przez producenta.
6. Wykonawca zobowiązuje się do monitorowania komunikatów producentów dotyczących podatności bezpieczeństwa dostarczonych urządzeń.

§ 5. KARY UMOWNE

1. Wykonawca zapłaci Zamawiającemu kary umowne:
 - a) za zwłokę w realizacji przedmiotu umowy – w wysokości 1% wynagrodzenia brutto za każdy dzień zwłoki;
 - b) za zwłokę w usunięciu wad w okresie gwarancji – w wysokości 0,5% wynagrodzenia brutto za każdy dzień zwłoki;
 - c) za odstąpienie od umowy przez którąkolwiek ze Stron z przyczyn leżących po jego stronie Wykonawcy w wysokości 20% wynagrodzenia brutto;
 - d) za naruszenie wymagań dotyczących bezpieczeństwa i cyberbezpieczeństwa określonych w umowie lub zapytaniu ofertowym, w tym w szczególności za niezastosowanie wymaganych mechanizmów zabezpieczeń, brak aktualizacji oprogramowania, niezgłoszenie incydentu bezpieczeństwa lub ujawnienie informacji poufnych, w wysokości 10% wynagrodzenia brutto za każde stwierdzone naruszenie;
 - e) za naruszenie przepisów dotyczących ochrony danych osobowych, zasad poufności lub postanowień Załącznika nr 8 – Umowy powierzenia przetwarzania danych osobowych i zobowiązania poufności – w wysokości 10% wynagrodzenia brutto za każde stwierdzone naruszenie.
 - f) Za brak zgłoszenia naruszenia ochrony danych osobowych lub incydentu bezpieczeństwa w terminach określonych w umowie lub Załączniku nr 8 Zamawiający może naliczyć karę umowną - w wysokości 5% wynagrodzenia brutto za każde naruszenie.
2. Zamawiający zastrzega sobie prawo do dochodzenia odszkodowania przewyższającego zastrzeżone kary umowne na zasadach ogólnych.
3. Zamawiający jest uprawniony do naliczania kar umownych bez uprzedniego wyznaczenia dodatkowego terminu do wykonania zobowiązania oraz do potrącania należnych kar z wynagrodzenia Wykonawcy lub z zabezpieczenia należytego wykonania umowy, o ile zostanie ustanowione.

§ 6. ODBIÓR ROBÓT

1. Podstawą odbioru jest protokół końcowego odbioru technicznego, podpisany przez obie strony. Zamawiający może dokonać odbioru z zastrzeżeniami, wskazując w protokole stwierdzone wady oraz termin ich usunięcia.
2. W razie stwierdzenia istotnych wad lub naruszeń wymagań bezpieczeństwa, w tym cyberbezpieczeństwa, Zamawiający jest uprawniony do odmowy podpisania protokołu odbioru do czasu ich usunięcia.
3. Odbiory częściowe mogą być przeprowadzane wyłącznie na wniosek Zamawiającego i nie stanowią one potwierdzenia kompletnego i zgodnego z umową wykonania całości przedmiotu umowy.
4. Do odbioru Wykonawca zobowiązany jest dostarczyć dokumentację powykonawczą (2 egz. papierowe + 1 PDF) oraz protokoły pomiarów elektrycznych.
5. Podczas odbioru końcowego sprawdzana będzie zgodność z parametrami określonymi w OPZ, jakość obrazu (dzień/noc) oraz poprawność nagrywania.
6. Warunkiem odbioru końcowego jest:
 - zmiana domyślnych haseł,
 - przekazanie logów systemowych,
 - przekazanie dokumentacji bezpieczeństwa,
 - wykonanie testów poprawności działania zabezpieczeń,
 - przekazanie kopii konfiguracji systemu.
7. Odbiór obejmuje również weryfikację:
 - konfiguracji uprawnień,
 - poprawności rejestracji logów,
 - retencji nagrań,
 - zabezpieczeń dostępu zdalnego.

§ 7. BEZPIECZEŃSTWO INFORMACJI I CYBERBEZPIECZEŃSTWO

1. Wykonawca zobowiązany jest do zaprojektowania, dostarczenia, skonfigurowania i uruchomienia systemu monitoringu w sposób zapewniający odpowiedni poziom bezpieczeństwa teleinformatycznego, w szczególności poprzez:
 - a) stosowanie aktualnych, wspieranych przez producenta wersji oprogramowania;
 - b) wdrożenie mechanizmów kontroli dostępu (m.in. indywidualne konta użytkowników, wymuszanie złożoności haseł, okresowa zmiana haseł);
 - c) szyfrowanie transmisji danych w sieci oraz zabezpieczenie kanałów zdalnego dostępu;
 - d) konfigurację urządzeń zgodnie z zasadą minimalnych uprawnień;
 - e) prowadzenie i udostępnienie Zamawiającemu dzienników zdarzeń (logów) umożliwiających odtworzenie działań użytkowników i incydentów bezpieczeństwa;
 - f) wdrożenie mechanizmów ochrony przed nieautoryzowaną ingerencją w urządzenia i oprogramowanie.
2. Wykonawca zapewnia, że wykorzystywane urządzenia i oprogramowanie są wolne od znanych luk bezpieczeństwa, które uniemożliwiałyby ich bezpieczną eksploatację, oraz że nie zawierają tzw. „tylnych furtek” umożliwiających nieautoryzowany dostęp.
3. W przypadku dostępu administracyjnego lub zdalnego Wykonawca zobowiązany jest do stosowania wieloskładnikowego uwierzytelniania (MFA), jeżeli urządzenia posiadają taką funkcjonalność.
4. System monitoringu nie może przekazywać obrazu, logów ani danych telemetrycznych do usług chmurowych producenta poza infrastrukturą Zamawiającego bez jego uprzedniej pisemnej zgody.
5. Wykonawca przekaże Zamawiającemu kopię konfiguracji systemu oraz procedurę odtworzenia konfiguracji po awarii.
6. Wykonawca zobowiązany jest do logicznego wydzielenia systemu monitoringu od sieci biurowej Zamawiającego z wykorzystaniem VLAN lub równoważnych mechanizmów separacji ruchu.

7. System monitoringu musi umożliwiać konfigurację okresów retencji nagrań zgodnie z obowiązującymi przepisami prawa oraz polityką ochrony danych osobowych Zamawiającego.
8. System powinien umożliwiać rejestrowanie dostępu do nagrań, eksportów materiałów oraz operacji wykonywanych przez użytkowników administracyjnych.
9. Wykonawca zobowiązany jest do niezwłocznego, nie później jednak niż w terminie 24 godzin od powzięcia wiadomości, zgłaszania Zamawiającemu wszelkich incydentów bezpieczeństwa dotyczących systemu monitoringu oraz do współpracy przy ich analizie i usuwaniu skutków.
10. W przypadku gdy incydent bezpieczeństwa dotyczy danych osobowych, zastosowanie mają również procedury określone w Załączniku do umowy.
11. Wykonawca przeprowadzi wstępne szkolenie wskazanych przez Zamawiającego użytkowników w zakresie bezpiecznej obsługi systemu, w tym zasad zarządzania uprawnieniami i reagowania na incydenty.

§ 8. POUFNOŚĆ

1. Wykonawca zobowiązuje się do zachowania w poufności wszelkich informacji uzyskanych w związku z realizacją niniejszej umowy, w tym informacji dotyczących infrastruktury technicznej Zamawiającego, konfiguracji systemu monitoringu, zabezpieczeń oraz zdarzeń rejestrowanych przez system.
2. Informacje, o których mowa w ust. 1, mogą być wykorzystywane wyłącznie w celu wykonania umowy i nie mogą być ujawniane osobom trzecim bez uprzedniej pisemnej zgody Zamawiającego, z wyjątkiem przypadków przewidzianych przepisami prawa.
3. Obowiązek zachowania poufności obowiązuje w czasie trwania umowy oraz po jej zakończeniu bez ograniczenia czasowego, chyba że przepisy prawa stanowią inaczej.
4. Jeżeli w związku z realizacją niniejszej umowy Wykonawca będzie przetwarzał dane osobowe w imieniu Zamawiającego, Strony zawrą odrębną umowę powierzenia przetwarzania danych osobowych, stanowiącą załącznik do niniejszej umowy.
5. Wykonawca zobowiązuje się do realizacji wszelkich obowiązków wynikających z przepisów o ochronie danych osobowych, w szczególności do stosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych przed ich utratą, zniszczeniem, nieuprawnionym dostępem lub ujawnieniem.
6. Informacje dotyczące infrastruktury technicznej, zabezpieczeń, konfiguracji systemów, logów oraz dokumentacji technicznej Zamawiającego stanowią informacje poufne o charakterze wrażliwym.
7. Po zakończeniu realizacji umowy Wykonawca zobowiązany jest do trwałego usunięcia wszelkich kopii danych i informacji pozyskanych podczas realizacji umowy.
8. Wykonawca nie jest uprawniony do wykorzystywania nagrań, logów, konfiguracji ani innych informacji pozyskanych podczas realizacji umowy do celów szkoleniowych, marketingowych, demonstracyjnych ani referencyjnych.
9. Postanowienia niniejszego paragrafu należy interpretować łącznie z Załącznikiem do umowy – Umową powierzenia przetwarzania danych osobowych i zobowiązaniem poufności.

§ 9. OCHRONA DANYCH OSOBOWYCH

1. Strony zobowiązują się do przestrzegania przepisów dotyczących ochrony danych osobowych, w szczególności:
 - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
 - ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
 - wewnętrznych procedur i polityk bezpieczeństwa obowiązujących u Zamawiającego.
2. W zakresie, w jakim realizacja niniejszej umowy wiąże się z przetwarzaniem danych osobowych przez Wykonawcę w imieniu Zamawiającego, zastosowanie mają postanowienia Załącznika do umowy – Umowy powierzenia przetwarzania danych osobowych stanowiącego integralną część niniejszej umowy.
3. Wykonawca zobowiązuje się do:

- przetwarzania danych wyłącznie w zakresie niezbędnym do realizacji umowy,
 - zapewnienia poufności danych osobowych,
 - stosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych,
 - zabezpieczenia danych przed nieuprawnionym dostępem, utratą, zniszczeniem lub ujawnieniem,
 - ograniczenia dostępu do danych wyłącznie do osób posiadających stosowne upoważnienia.
4. Wykonawca zobowiązuje się do niezwłocznego poinformowania Zamawiającego o każdym:
- naruszeniu ochrony danych osobowych,
 - incydencie bezpieczeństwa mogącym wpływać na bezpieczeństwo danych,
 - żądaniu udostępnienia danych otrzymanym od organów lub osób trzecich, chyba że zakaz poinformowania wynika z przepisów prawa.
5. Po zakończeniu realizacji umowy Wykonawca zobowiązany jest do:
- usunięcia danych osobowych i ich kopii,
 - usunięcia kont serwisowych i dostępu technicznych,
 - zwrotu nośników zawierających dane, jeżeli zostały przekazane przez Zamawiającego, zgodnie z postanowieniami Załącznika do umowy.
6. Zamawiający ma prawo do weryfikacji sposobu realizacji obowiązków wynikających z ochrony danych osobowych, w tym poprzez audyt lub żądanie przedstawienia stosownych informacji i dokumentów.
7. Naruszenie obowiązków określonych w niniejszym paragrafie stanowi istotne naruszenie umowy i może stanowić podstawę do:
- odmowy odbioru,
 - naliczenia kar umownych,
 - odstąpienia od umowy,
 - dochodzenia odszkodowania na zasadach ogólnych.

§ 10. GOSPODARKA ODPADAMI

Wykonawca zobowiązany jest do zagospodarowania odpadów powstałych w wyniku demontażu istniejących kamer i urządzeń zgodnie z ustawą o odpadach, ustawą o zużyтым sprzęcie elektrycznym i elektronicznym oraz postanowieniami zapytania ofertowego.

§11. AUDYT I KONTROLA

1. Zamawiający ma prawo przeprowadzenia audytu bezpieczeństwa dotyczącego realizacji niniejszej umowy.
2. Audyt może obejmować również weryfikację zgodności przetwarzania danych osobowych z RODO oraz postanowieniami Załącznika do umowy.
3. Wykonawca zobowiązany jest do współpracy podczas audytu, w szczególności do:
 - udostępnienia dokumentacji,
 - przedstawienia konfiguracji systemu,
 - przedstawienia logów,
 - przedstawienia informacji o zastosowanych zabezpieczeniach.
4. W przypadku stwierdzenia niezgodności Wykonawca zobowiązany jest do ich usunięcia w terminie wskazanym przez Zamawiającego.

§12. ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

1. Wykonawca zobowiązuje się do stosowania środków organizacyjnych i technicznych odpowiadających wymaganiom normy ISO/IEC 27001.
2. W szczególności Wykonawca zapewni:
 - kontrolę dostępu,

- zarządzanie podatnościami,
- ochronę przed malware,
- aktualizacje bezpieczeństwa,
- rejestrowanie zdarzeń,
- ciągłość działania systemu.

§13. WYMAGANIA ENERGETYCZNE

1. Wykonawca zobowiązuje się do stosowania urządzeń energooszczędnych oraz konfiguracji ograniczającej zużycie energii elektrycznej.
2. Dostarczone urządzenia powinny wspierać funkcje zarządzania energią i być dostosowane do pracy ciągłej 24/7 w infrastrukturze energetycznej Zamawiającego.

§ 14. POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu cywilnego oraz zapisy zapytania ofertowego.
2. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach – po jednym dla każdej ze stron.
3. Wykonawca zobowiązany jest do realizacji przedmiotu umowy zgodnie z wymaganiami cyberbezpieczeństwa określonymi w zapytaniu ofertowym, w tym w zakresie konfiguracji, szyfrowania, aktualizacji i szkoleń.
4. Zmiana niniejszej Umowy wymaga formy pisemnej pod rygorem nieważności.
5. W przypadku powstania sporu na tle wykonania niniejszej Umowy sądem powszechnym właściwym do jego rozstrzygnięcia będzie sąd właściwy dla Zamawiającego.
6. Załącznik do umowy – Umowa powierzenia przetwarzania danych osobowych i zobowiązanie poufności stanowi integralną część niniejszej umowy.

ZAMAWIAJĄCY

.....

podpis i pieczęć

WYKONAWCA

.....

podpis i pieczęć