UMOWA nr ……(wzór)

zawarta w Olsztynie w dniu ..... w wyniku postępowania o udzielenie zamówienia realizowanego zgodnie zapisami art. 6a ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843 ze zm.) pomiędzy:

Województwem Warmińsko-Mazurskim z siedzibą w Olsztynie przy ul. Emilii Plater 1, 10-562 Olsztyn /NIP: 7393890447; zwanym dalej **Zamawiającym**, reprezentowanym przez Zarząd Województwa Warmińsko-Mazurskiego, w imieniu którego działają:

1. ……

2. ……..……

a
…… z siedzibą w ……. przy …….., NIP: ……., REGON: ……., zwanym dalej **Wykonawcą**, w imieniu którego działają:

1. ……

zaś łącznie zwanymi dalej **Stronami**.

§1

1. Przedmiotem umowy jest usługa dostarczenia i wdrożenia systemu do nadzorowania dostępu do zasobów teleinformatycznych Urzędu Marszałkowskiego WWM w Olsztynie Województwa Warmińsko-Mazurskiego w Olsztynie, wraz z 12 miesięcznym wsparciem serwisowym.
2. Wykonawca oświadcza, że przysługują mu prawa do rozporządzania licencją na system do nadzorowania dostępu do zasobów teleinformatycznych nadane przez producenta systemu (gwaranta).
3. Wykonawca zobowiązany jest do przekazania Zamawiającemu wymaganych licencji niezbędnych do prawidłowego i zgodnego ze szczegółowym opisem przedmiotu zamówienia.
4. Szczegółowy opis przedmiotu zamówienia opisany jest w załączniku nr 1 do umowy.

§2

1. Wykonawca zobowiązuje się do rozpoczęcia świadczenia usługi, o której mowa w § 1 ust. 1 umowy, w terminie do 5 dni od dnia zawarcia niniejszej umowy.
2. Wykonawca zobowiązuje się do zakończenia wdrożenia do dnia ……..2020 r.
3. Z odbioru przedmiotu umowy zostanie sporządzony protokół odbioru końcowego podpisany przez obie strony bez zastrzeżeń. Osobą uprawnioną ze strony Zamawiającego do jednoosobowego podpisania protokołu odbioru, niezależnie od osób uprawnionych do reprezentowania Zamawiającego, jest: …….. lub ……..
4. Za termin odbioru przedmiotu umowy przyjmuje się datę potwierdzoną przez Zamawiającego i Wykonawcę na protokole, o którym mowa w § 2 ust. 3.
5. Podstawą wystawienia faktury VAT/rachunku jest podpisanie przez Zamawiającego protokołu odbioru końcowego bez zastrzeżeń, stwierdzającego przekazanie Zamawiającemu przedmiotu umowy zgodnego z wymaganiami.

§3

1. Całkowite wynagrodzenie Wykonawcy z tytułu należytego wykonania przedmiotu umowy wynosi …….. zł brutto, słownie (……..……..), w tym należny podatek VAT.
2. Wynagrodzenie Wykonawcy za wykonanie przedmiotu umowy, wskazane w § 3 ust. 1, jest niezmienne, zawiera w sobie wszystkie koszty Wykonawcy związane z prawidłową realizacją umowy i zaspokaja wszelkie roszczenia Wykonawcy wobec Zamawiającego z tytułu wykonania umowy.
3. Wynagrodzenie przysługujące Wykonawcy zostanie wypłacone na podstawie prawidłowo wystawionej przez Wykonawcę faktury VAT/rachunku w terminie 21 dni od dnia jej dostarczenia do siedziby Zamawiającego, na rachunek bankowy Wykonawcy o numerze …… . Termin uważa się za zachowany, jeżeli przed jego upływem zostanie wydana dyspozycja obciążenia rachunku bankowego Zamawiającego.
4. Wykonawca wystawi fakturę VAT/rachunek. Faktura VAT/rachunek winna zawierać następujące dane:
   Nabywca: Województwo Warmińsko-Mazurskie w Olsztynie, ul. Emilii Plater 1, 10-562 Olsztyn, NIP 739-38-90-447,
   Odbiorca: Urząd Marszałkowski Województwa Warmińsko-Mazurskiego w Olsztynie, ul. Emilii Plater 1, 10-562 Olsztyn.
5. W przypadku wystawienia przez Wykonawcę faktury elektronicznej dane do przekazania takiej faktury Zamawiający przekaże na wniosek Wykonawcy.
6. W przypadku gdy dane, wymienione na fakturze VAT/rachunku będą błędne, Zamawiający odmówi przyjęcia faktury VAT/rachunku, a termin określony w § 3 ust. 3 nie będzie rozpoczęty, na co Wykonawca wyraża zgodę.
7. W przypadku opóźnienia w dokonaniu płatności Wykonawca może obciążyć Zamawiającego ustawowymi odsetkami za opóźnienie.

§4

1. W razie zaistnienia 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 istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach. W takim wypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.
2. Zamawiający może odstąpić od umowy z przyczyn leżących po stronie Wykonawcy w terminie 21 dni od dnia powzięcia wiadomości o tych przyczynach, lecz nie później niż w terminie 30 dni następujących po upływie terminu określonego w § 2 ust.1 umowy.
3. Wykonawca może odstąpić od umowy z przyczyn leżących po stronie Zamawiającego w terminie 21 dni od dnia powzięcia wiadomości o tych przyczynach, lecz nie później niż w terminie 30 dni następujących po upływie terminu określonego w § 2 ust.1 umowy.
4. Odstąpienie od umowy którejkolwiek ze stron wymaga formy pisemnej pod rygorem nieważności oraz wymaga uzasadnienia.

§ 5

1. Okres gwarancji wynosi 12 miesięcy licząc od dnia odbioru przedmiotu umowy potwierdzonego protokołem odbioru podpisanym przez Zamawiającego. Zgłoszenia usterek dokonywane będą

telefonicznie: ……,: ……..... lub pocztą elektroniczną: …….. Przyjmowanie zgłoszeń serwisowych wad i usterek oprogramowania będzie mogło następować przez 24 godziny na dobę, przez 7 dni w tygodniu przez wszystkie dni w roku. Za chwilę zgłoszenia wad lub usterek uważa się odpowiednio chwilę zgłoszenia wad lub usterek oprogramowania telefonicznie, pocztą elektroniczną pod numerem telefonu/adresem poczty elektronicznej, o którym mowa wyżej.

2. Gwarant zobowiązuje się dokonywać naprawy oprogramowania lub wymiany na nowe, wolne od wad w przypadku wystąpienia uszkodzeń powstałych na skutek niewłaściwej budowy, wad ukrytych lub wystąpienia innych niesprawności dostarczonego oprogramowania.
3. Naprawy gwarancyjne świadczone będą u Zamawiającego, zdalnie lub w miejscu użytkowania przedmiotu umowy.
4. Naprawa oprogramowania (rozumiana jako usunięcie wad, usterek) nastąpi niezwłocznie, nie później jednak niż w terminie 3 dni, liczonych od dnia zgłoszenia.
5. Gwarant nie może żądać od Zamawiającego jakichkolwiek dodatkowych świadczeń, opłat lub kosztów, a także żądać od Zamawiającego wypełniania dodatkowych obowiązków lub ograniczać Zamawiającego w jego prawach wynikających z zapisów umowy z tytułu udzielanej gwarancji i świadczonych w jej ramach napraw gwarancyjnych.
6. Wykonawca zobowiązuje się do wykonywania obowiązków wynikających z Umowy w sposób zapobiegający utracie danych Zamawiającego, do których będzie miał dostęp w trakcie wykonywania prac. W przypadku, gdy wykonywanie prac wiąże się z ryzykiem utraty danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego przed przystąpieniem do naprawy oraz umożliwić Zamawiającemu wykonanie kopii zapasowych danych.
7. Zamawiający ma prawo wykonywać uprawnienia z tytułu rękojmi za wady oprogramowania niezależnie od uprawnień wynikających z gwarancji.
8. Gwarant ponosi wszelkie koszty napraw gwarancyjnych, włączając w to koszt części i transportu.

§6

1. W przypadku zwłoki w wykonaniu przedmiotu umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,4 % całkowitego wynagrodzenia brutto, określonego w § 3 ust. 1 umowy, za każdy dzień zwłoki, licząc od dnia następującego po upływie terminu określonego w § 2 ust. 2 umowy. Łączna wysokość kary umownej, o której mowa w niniejszym ustępie nie może przekroczyć 10 % kwoty wynagrodzenia brutto określonego w § 3 ust. 1 umowy.
2. W przypadku nieuzasadnionego odstąpienia od umowy przez Wykonawcę lub odstąpienia od umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10 % całkowitego wynagrodzenia brutto określonego w § 3 ust. 1 umowy.
3. W przypadku nieuzasadnionego odstąpienia od umowy przez Zamawiającego lub odstąpienia od umowy przez Wykonawcę z przyczyn leżących po stronie Zamawiającego, Zamawiający zapłaci Wykonawcy karę umowną w wysokości 10 % całkowitego wynagrodzenia brutto określonego w § 3 ust. 1 umowy.
4. Strony zobowiązane są do zapłacenia kar umownych w terminie 21 dni od dnia otrzymania noty obciążeniowej wystawionej z tego tytułu przez drugą stronę. Termin uważa się za zachowany, jeżeli przed jego upływem zostanie wydana dyspozycja obciążenia rachunku bankowego Strony zobowiązanej do zapłaty kary.
5. Zamawiający zastrzega sobie możliwość potrącenia kar umownych z wynagrodzeniem przysługującym Wykonawcy.
6. Strony mogą dochodzić na zasadach ogólnych odszkodowania przekraczającego wysokość zastrzeżonych kar umownych.

§7

W przypadku, o którym mowa w § 6 ust. 1 umowy, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.

§8

1. W sprawach realizacji umowy strony porozumiewają się za pośrednictwem telefonu, poczty elektronicznej.
2. Wykonawca, w terminie 3 dni roboczych od dnia zawarcia umowy przekaże Zamawiającemu dane kontaktowe osoby lub osób wyznaczonych do merytorycznej współpracy i koordynacji w wykonywaniu umowy, zawierające: imię i nazwisko, nr telefonu, adres poczty elektronicznej.
3. W przypadku, gdy Wykonawca nie przekaże danych, o których mowa w § 8 ust. 2, Zamawiający, w sprawach realizacji umowy, wykorzysta dane kontaktowe Wykonawcy zawarte w ofercie.
4. Osobami wyznaczonymi do merytorycznej współpracy i koordynacji w wykonywaniu umowy ze strony Zamawiającego są:....., tel.: ……, adres e-mail.: ……
5. Zmiana osób, o których mowa w § 8 ust. 2 i 4 następuje poprzez pisemne powiadomienie drugiej strony i nie stanowi zmiany treści umowy.

§9

1. Informacje, w posiadanie których Wykonawca wejdzie w związku z realizacją umowy będą traktowane przez Wykonawcę jako poufne w czasie obowiązywania umowy oraz do dwóch lat od momentu jej wykonania, rozwiązania, wygaśnięcia i odstąpienia od niej i mogą być ujawniane wyłącznie tym osobom i upoważnionym przedstawicielom, których obowiązkiem jest realizacja umowy, pod rygorem pociągnięcia Wykonawcy do odpowiedzialności za naruszenie poufności.
2. Wykonawca zobowiązuje się do zachowania w poufności informacji, o których mowa w ust. 1, w szczególności:
   - nieujawniania i niezezwalania na ujawnienie jakichkolwiek informacji poufnych w jakiejkolwiek formie w całości lub w części jakiejkolwiek osobie trzeciej bez uprzedniej zgody Zamawiającego wyrażonej na piśmie pod rygorem nieważności;
   - zapewnienia, że personel oraz inni współpracownicy Wykonawcy, którym informacje, o których mowa w ust. 1 zostaną udostępnione nie ujawnią i nie zezwolą na ich ujawnienie w jakiejkolwiek formie w całości lub w części jakiejkolwiek osobie trzeciej bez uprzedniej zgody Zamawiającego wyrażonej na piśmie pod rygorem nieważności;
   - zapewnienia prawidłowej ochrony informacji przed utratą, kradzieżą, zniszczeniem, zgubieniem lub dostępem osób trzecich nieupoważnionych do uzyskania informacji, o których mowa w ust. 1;
   - niewykorzystywania informacji, o których mowa w ust. 1, do innych celów niż wykonywanie czynności wynikających z umowy bez uprzedniej zgody Zamawiającego wyrażonej pisemnie pod rygorem nieważności.
3. Wykonawca zobowiązuje się do przejęcia na siebie wszelkich roszczeń osób trzecich w stosunku do Zamawiającego, wynikających z wykorzystania informacji uzyskanych w związku z realizacją umowy w sposób naruszający jej postanowienia.
4. Wykonawca zobowiązuje się do niezwłocznego zawiadomienia Zamawiającego o każdym przypadku ujawnienia informacji, o których mowa w ust. 1, pozostającym w sprzeczności z postanowieniami umowy.
5. Zobowiązanie do zachowania poufności informacji, o których mowa w ust. 1 nie dotyczy przypadków, gdy informacje te:
   - stały się publicznie dostępne, jednak w inny sposób niż w wyniku naruszenia umowy;

- muszą zostać udostępnione zgodnie z obowiązkiem wynikającym z przepisów powszechnie obowiązującego prawa, orzeczenia sądu lub uprawnionego organu administracji publicznej; w takim przypadku Wykonawca będzie zobowiązany zapewnić, by udostępnienie informacji, o których mowa w ust. 1 nastąpiło tylko i wyłącznie w zakresie koniecznym dla zadośćuczynienia powyższemu obowiązkowi.

6. Wykonawca niezwłocznie zawiadomi Zamawiającego o każdym przypadku zaistnienia obowiązku udostępnienia informacji, o których mowa w ust. 1, a także podejmie wszelkie działania konieczne do zapewnienia, by udostępnienie informacji, o których mowa w ust. 1 dokonało się w sposób chroniący przed ujawnieniem ich osobom niepowołanym.
7. Zamawiający, jako administrator danych osobowych, upoważnia Wykonawcę do ich przetwarzania tylko i wyłącznie w celu właściwego wykonania Umowy, zgodnie z warunkami określonymi w Umowie powierzenia przetwarzania danych osobowych, stanowiącej załącznik nr 2 do niniejszej Umowy. Umowa powierzenia przetwarzania danych osobowych zwarta jest w oparciu o przepis art. 28 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

§ 10

1. W sprawach nieuregulowanych niniejszą umową wiąże oferta Wykonawcy, postanowienia zawarte w opisie warunków zamówienia, a także stosuje się przepisy ustawy Prawo zamówień publicznych, kodeksu cywilnego oraz aktów wykonawczych do tych ustaw.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
3. Właściwym do rozpoznania sporów wynikłych na tle realizacji niniejszej umowy jest polski sąd powszechny właściwy miejscowo dla siedziby Zamawiającego oraz prawo polski.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach w tym jeden dla Zamawiającego i jeden dla Wykonawcy.

Zamawiający **Wykonawca**

Załącznik nr 1 do Umowy

Szczegółowy opis przedmiotu zamówienia

Usługa wdrożenia systemu do nadzorowania dostępu do zasobów teleinformatycznych Urzędu Marszałkowskiego Województwa Warmińsko-Mazurskiego w Olsztynie

W ramach postępowania wymagane jest dostarczenie, skonfigurowanie oraz uruchomienie rozwiązania służącego do nadzorowania dostępu dla co najmniej 300 stacji roboczych do zasobów teleinformatycznych Urzędu. Wdrożenie musi być przeprowadzone przez inżynierów posiadających certyfikaty NSE 4,5 i 7 (kopie certyfikatów załączone do oferty).

Dostarczone rozwiązanie musi być kompatybilne w 100% z posiadanym przez zamawiającego urządzeniem FortiGate 600D oraz FortiAnalizer 400E, które są obecnie i będą w przyszłości objęte wsparciem serwisowym producenta. Dotyczy to zarówno obecnej wersji firmware jak i przyszłych, które zostaną przez producenta wydane. Oferowane rozwiązanie musi posiadać centralne zarządzanie zainstalowanym na stacjach roboczych oprogramowaniem.

Parametry systemu ochrony dla stacji roboczych.

1. Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy:
   a. Kontrola antywirusowa.
   b. URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
   c. Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny.
   d. Mechanizmy analizy podatności na stacji roboczej pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
   e. Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
   f. Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
   g. Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
   h. Mechanizmy uwierzytelniania dwuskładnikowego.
   i. Funkcję blokowania urządzeń USB.
2. Poszczególne mechanizmy muszą być dostępne dla następujących wersji systemów operacyjnych Windows oraz Mac OS: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Mac OS X v10.14, OS X v10.13, OS X v10.12.
3. Wymaganym jest aby system ochrony stacji końcowej (co najmniej dla tych z systemem operacyjnym Windows) miał możliwość wysyłania plików do platformy typu Sandbox zlokalizowanej w chmurze producenta (co najmniej w ilości 300 plików dziennie dla każdej stacji roboczej).

Parametry systemu centralnego zarządzania.

1. Dostarczony system centralnego zarządzania zainstalowanym na stacjach roboczych oprogramowaniem musi zapewniać wszystkie wymienione poniżej funkcje.
2. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019, Microsoft Windows Server 2016. Zamawiający udostępni zasoby w poosiadanym przez siebie środowisku wirtualnym opartym na rozwiązaniach firmy VMware w postaci:
   - zasoby dyskowe do 500 GB,
   - pamięć RAM do 32 GB,
   - CPU do 12 rdzeni,
   - karta sieciowa – 2 x 1Gb/s
   - licencja Windows Server 2016 Data Center

3. System musi umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox.
4. Ponadto wymagane jest aby system zapewniał:
   a. Integrację z systemami zarządzania tożsamością użytkowników –Active Directory.
   b. Definiowanie różnych profili (wersji konfiguracji) ochrony dla różnych grup użytkowników pobieranych z AD lub definiowanych lokalnie.
   c. Zautomatyzowany proces zarządzania aplikacją kliencką.
   d. Przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS, w których administrator może określić komponenty dla ochrony stacji roboczych takie jak :
      - kontrola antywirusowa,
      - filtrowanie URL,
      - analiza podatności.
   e. Możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym.
   f. Panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych.
   g. Panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych.
   h. Możliwość wymuszenia uaktualniania/łatania wykrytych podatności na stacjach roboczych.
   i. Automatyczne wykrywanie stacji klienckich w grupach roboczych.
   j. Logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcją filtrów oraz możliwością pobierania logów przez administratora.
   k. Generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji typu botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa.
   l. Definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego.
   m. Zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN.
   n. Automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji.
   o. Możliwość przeniesienia użytkownika do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi.
   p. Możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,
   q. Możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces.
5. Administrator musi mieć możliwość wykonywania backupu i odtwarzania danych zgromadzonych w oferowanym rozwiązaniu.
6. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.

Licencje oraz serwisy.

W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające co najmniej do:

1. Zainstalowania i centralnego zarządzania aplikacjami klienckimi na minimum 300 stacjach roboczych. W ramach umowy Wykonawca zobowiązany będzie do przeprowadzenia przykładowego wdrożenia na maksymalnie 10 stacjach roboczych wyposażonych w system MS Windows i na maksymalnie 3 stacjach wyposażonych w system Mac OS.
2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować:
   a. Kontrolę aplikacji,
   b. System Antywirusowy,
   c. Web Filtering,

d. Skaner podatności,
e. Software inventory,
f. Remote Access,
g. Threat Outbreak Detection,
h. Sandbox Agent with Cloud Sandbox subscription – co najmniej 300 plików dziennie dla każdej z nadzorowanych stacji roboczych.

3. System musi być objęty serwisem producenta przez okres co najmniej 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7 realizowanym zarówno przez producenta rozwiązania jak i Wykonawcę.
4. Wykonawca zapewni wsparcie powdrożeniowe inżynierów posiadających certyfikat NSE 4,5 i 7 (kopie certyfikatów załączone do oferty) w ilości co najmniej 30 roboczogodzin obejmujące co najmniej :
   - możliwość konsultacji telefonicznych,
   - możliwość konsultacji z wykorzystaniem telekonferencji,
   - możliwość konsultacji z wykorzystaniem zdalnego dostępu do infrastruktury Zamawiającego.

Załącznik nr 2 do Umowy

Oznaczenie administratora danych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Olsztyn, dnia …… r.

UPOWAŻNIENIE NR ……

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1), **upoważniam**:

Panią/Pana.....
/imię i nazwisko/

zatrudnioną/nego w .....
/nazwa/

do przetwarzania danych osobowych w zbiorze .....
/nazwa zbioru danych osobowych/

w zakresie.....
/ np. kategorie danych, operacje na danych osobowych, jakich może dokonywać osoba upoważniona do przetwarzania danych osobowych/

Sposób przetwarzania danych osobowych: zautomatyzowany*/niezautomatyzowany*

Niniejsze upoważnienie jest ważne od dnia ……do dnia……* / do odwołania

lub ustania zatrudnienia w ……..…....

……
Administrator Danych

* należy wybrać właściwe