Załącznik nr 5 do zapytania ofertowego

Umowa nr ……. /2022

zawarta w dniu ..... 2022 r. pomiędzy:
Gminą Lipce Reymontowskie z siedzibą w Lipcach Reymontowskich przy ul. Reymonta 24, 96-127 Lipce Reymontowskie, NIP 833-10-91-147, REGON 750148302
reprezentowaną przez:
Wójta Gminy Lipce Reymontowskie – Marka Sałka
przy kontrasygnacie **Skarbnika Gminy – Joanny Karpowiak** -
zwaną w dalszej części umowy **„Zamawiającym"**
a
***…… prowadzącym działalność gospodarczą pod firmą …… z głównym zakładem pod adresem: ……, zamieszkałym w …… przy ul. ……, NIP: ……, REGON: ……, PESEL: ……**
***…… z siedzibą w ……, przy ul. ……, wpisaną do rejestru prowadzonego przez Sąd Rejonowy ……, …… Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: ……, NIP: ……, REGON……**
reprezentowanym przez:
……, zwanym w dalszej części umowy **„Wykonawcą".**
o następującej treści:

Oświadczenia stron

1. Strony oświadczają, że niniejsza umowa, zwana dalej „umową", została zawarta w wyniku rozstrzygnięcia zapytania ofertowego. Zamawiający oświadcza, że przy wyborze Wykonawcy nie miały zastosowania przepisy ustawy z dnia z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jedn. Dz. U. z 2021r poz. 1129 z późn. zm.) zgodnie z art. 2 ust. 1 pkt. 1 ustawy.

2. Zamawiający oświadcza, iż zadanie, o którym mowa w § 1 umowy współfinansowane jest ze środków pochodzących z Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00.

§ 1
Przedmiot umowy

1. Przedmiotem za zamówienia jest przeprowadzenie diagnozy cyberbezpieczeństwa oraz przeprowadzenie stacjonarnego szkolenia w zakresie cyfrowego bezpieczeństwa informacji w Urzędzie Gminy Lipce Reymontowskie.

2. Przedmiot zamówienia musi być przeprowadzony zgodnie ze Szczegółowym Opisem Przedmiotu Zamówienia stanowiącym Załącznik nr 1 do umowy.

3. Diagnoza cyberbezpieczeństwa musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa" stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina.

4. Diagnoza cyberbezpieczeństwa musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

5. Zamówienie jest współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

§ 2
Termin realizacji umowy

1. Wykonawca zrealizuje przedmiot umowy nie później niż w ciągu 1 miesiąca od daty zawarcia umowy.
2. Za datę zawarcia umowy Zamawiający przyjmuje dzień, w którym zostanie ona podpisana przez obie Strony umowy.

§ 3
Obowiązki stron

1. Strony umowy zobowiązują się do pełnej współpracy w ramach realizowanego zlecenia, opartej na wzajemnym zaufaniu.
2. W związku z intencją Stron określoną w ust. 1 Wykonawca zobowiązuje się świadczyć usługi objęte umową z należytą starannością, zgodnie z obowiązującymi przepisami prawa, zobowiązując się do składania wszelkich wyjaśnień Zamawiającemu w trakcie realizacji umowy.
3. Opracowania wykonane w ramach niniejszej umowy przez Wykonawcę, muszą być zgodne z dokumentacją konkursu grantowego Cyfrowa Gmina, w tym Wzorem umowy o powierzenie grantu, w szczególności z celem i przeznaczeniem wskazanymi w ustępie poniżej.
4. Zamawiający jest zobowiązany do przekazania wyników diagnozy do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z diagnozy przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca potwierdza, że ma świadomość wyżej wskazanego celu przeprowadzenia diagnozy i jej przeznaczenia.
5. Wykonawca wykona niniejszą umowę m.in. w oparciu o informacje pozyskane przez Wykonawcę w toku jej realizacji, dostarczone przez Zamawiającego oraz decyzje przez niego podjęte w trakcie realizacji umowy.
6. Zamawiający udostępni Wykonawcy wszelkie niezbędne informacje i dokumenty do świadczenia usług będących przedmiotem niniejszej umowy.
7. Wykonawca zobowiązuje się, że wszystkie dokumenty i inne materiały, w których posiadanie wejdzie w związku z wykonywaniem niniejszej umowy pozostaną własnością Zamawiającego. Wykonawca zwróci je właścicielowi nie później niż w dniu rozwiązania lub wygaśnięcia niniejszej umowy.
8. Prace związane z pozyskaniem informacji, dokumentów i innych materiałów niezbędnych do przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa oraz diagnozy cyberbezpieczeństwa będą wykonywane w siedzibie Zamawiającego.
9. Wykonawca przekaże wynik przeprowadzonej diagnozy w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w §1 ust. 3, podpisanego podpisem cyfrowym (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia, o których mowa w ust. §1 ust. 4.
10. W przypadku, jeśli beneficjent projektu „Cyfrowa Gmina" tj. Centrum Projektów Polska Cyfrowa zmodyfikuje plik formularza, o którym mowa w powyższym ustępie, Wykonawca przekaże wynik diagnozy sporządzony w oparciu o aktualną wersję pliku. W dniu podpisania umowy plik formularza jest dostępny pod adresem https://www.gov.pl/web/cppc/cyfrowa-gmina, sekcja „Dokumentacja konkursowa" / "Regulamin Konkursu".
11. W celu uniknięcia wątpliwości przyjmuje się, że jeżeli Strony nie zdefiniowały danego działania niezbędnego do prawidłowej realizacji umowy jako obowiązku Zamawiającego, Stroną zobowiązaną do wykonania takiego działania jest Wykonawca jako podmiot profesjonalny.
12. Zamawiający w każdym czasie trwania umowy, ma prawo do kontroli prawidłowości wykonywania obowiązków przez Wykonawcę. Jeśli w trakcie realizacji umowy Zamawiający zauważy lub podejrzewać będzie przyjęcie nieprawidłowych założeń lub podjęcie niewłaściwej decyzji przez Wykonawcę, niezwłocznie przekaże Wykonawcy odpowiednią pisemną informację w tym zakresie oraz zaproponuje stosowne rozwiązanie stwierdzonych nieprawidłowości.
13. Zamawiający nie zezwala Wykonawcy na powierzenie wykonania prac objętych niniejszą umową osobom trzecim.

14. Strony umowy postanawiają, że Wykonawcy nie można postawić zarzutu braku należytej staranności przy realizacji prac jeżeli te okoliczności wynikają z:

    1) działania sił przyrody,

    2) działania lub zaniechania organów państwowych i samorządowych polegających m.in. na zmianie przepisów prawnych,

    3) nie udzielenia informacji bądź nie udostępnienia Wykonawcy przez Zamawiającego dokumentów istotnych z punktu widzenia realizacji przedmiotu umowy.

15. Prawa i obowiązki Stron określone i wynikające z niniejszej umowy nie mogą być przenoszone na osoby trzecie.

§ 4
Wynagrodzenie

1. Za wykonanie przedmiotu umowy, określonego w §1 niniejszej umowy, Strony ustalają wynagrodzenie ryczałtowe w wysokości ……. zł brutto (słownie: ……..) w tym wartość podatku od towarów i usług: ……..…… zł według stawki ….. % oraz wartość netto: ……..…… zł, zgodnie z ofertą Wykonawcy.

2. Wynagrodzenie, o którym mowa w ust. 1 pozostaje niezmienne i nie podlega waloryzacji przez okres realizacji umowy, również bez względu na ewentualne zmiany umowy w zakresie terminu realizacji związane z zakończeniem lub przesunięciem terminu zakończenia projektu.

3. Wynagrodzenie płatne będzie jednorazowo, na rachunek bankowy Wykonawcy wskazany na fakturze po wykonaniu niżej wymienionych etapów przedmiotu umowy, tj.

    1) przeprowadzenie diagnozy cyberbezpieczeństwa,

    2) przeprowadzenie szkolenia dla urzędników w zakresie cyberbezpieczeństwa.

4. Strony ustalają, że podstawą do wystawienia przez Wykonawcę faktury jest należyte wykonanie obowiązków Wykonawcy wynikających z niniejszej umowy, potwierdzone protokołem odbioru każdego z etapów przedmiotu umowy, podpisanym przez Zamawiającego bez zastrzeżeń.

5. Wynagrodzenie płatne będzie w terminie do 14 dni od daty złożenia przez Wykonawcę prawidłowo wystawionej faktury w siedzibie Zamawiającego.

6. Za datę zapłaty przyjmuje się dzień obciążenia przez bank rachunku Zamawiającego. Termin uważa się za zachowany, jeżeli obciążenie rachunku bankowego Zamawiającego nastąpi najpóźniej w ostatnim dniu terminu płatności.

7. Zamawiający zastrzega sobie prawo rozliczania płatności wynikającej z Umowy z zastosowaniem mechanizmu podzielnej płatności, przewidzianego w przepisach ustawy o podatku od towarów i usług.

8. Wykonawca oświadcza, ze rachunek bankowy Wykonawcy:

    1) jest rachunkiem umożliwiającym płatność z zastosowaniem mechanizmu podzielnej płatności, o którym mowa powyżej,

    2) znajduje się w wykazie podmiotów prowadzonym przez Szefa Krajowej Administracji Skarbowej, o którym mowa w art. 96b ustawy o podatku od towarów i usług (tzw. biała lista podatników).

9. W przypadku, gdy rachunek bankowy Wykonawcy nie spełnia choćby jednego z warunków określonych w pkt. 8, opóźnienie w dokonaniu płatności w terminie określonym w umowie, powstałe wskutek braku możliwości:

    1) realizacji przez Zamawiającego płatności wynagrodzenia z zastosowaniem mechanizmu podzielnej płatności i/lub

    2) dokonania płatności na rachunek objęty wykazem podmiotów prowadzonym przez Szefa Krajowej Administracji Skarbowej,

    nie stanowi dla Wykonawcy podstawy do żądania od Zamawiającego jakichkolwiek odsetek/odszkodowań lub innych roszczeń z tytułu dokonania nieterminowej płatności.

§ 5
Odstąpienie od umowy

1. Jeśli Wykonawca w rażący sposób narusza postanowienia umowy, Zamawiający może odstąpić od umowy w ciągu 30 dni po upływie wyznaczonego dodatkowego 7-dniowego terminu zawierającego wezwanie do prawidłowego wykonywania obowiązków wynikających z zawartej umowy, jeżeli Wykonawca pomimo upływu dodatkowego terminu w dalszym ciągu w sposób rażący narusza postanowienia umowy.
2. Zamawiający może również odstąpić od umowy, o ile Wykonawca wykonuje umowę wadliwie lub w sposób sprzeczny z umową, niezgodnie ze złożona ofertą lub realizuje umowę niedbale, niezgodnie z dokonanymi uzgodnieniami z zastosowaniem takiej samej procedury i terminu odstąpienia jak wskazane w ust. 1.
3. Zamawiający może również odstąpić od umowy ze skutkiem natychmiastowym, jeżeli Wykonawca nie dotrzymał terminu, o którym mowa w §2 ust. 1. Odstąpienie z przyczyn wskazanych w zdaniu pierwszym może nastąpić w terminie 30 dni od powzięcia informacji o istnieniu podstawy do odstąpienia od umowy.
4. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 7 dni od daty powzięcia wiadomości o tych okolicznościach. W takim przypadku Wykonawca może żądać jedynie wynagrodzenia należnego z tytułu wykonania części umowy.
5. Odstąpienie od umowy wymaga formy pisemnej pod rygorem nieważności.

§ 6
Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne w następujących przypadkach:
   1) za odstąpienie od umowy przez Zamawiającego z przyczyn, o których mowa w § 5 ust. od 1 do 3 oraz z innych przyczyn, za które odpowiedzialność ponosi Wykonawca, w wysokości 20% całkowitego wynagrodzenia brutto określonego w § 4 ust. 1;
   2) za odstąpienie od umowy przez Wykonawcę w wysokości 20% całkowitego wynagrodzenia brutto określonego w § 4 ust. 1;
   3) za zwłokę w wykonaniu przedmiotu umowy w wysokości 2% wynagrodzenia brutto określonego w § 4 ust. 1, za każdy rozpoczęty dzień zwłoki, licząc od upływu terminu wskazanego § 2 ust. 1 w umowie.

2. Zamawiający zapłaci Wykonawcy karę umowną za:

1) za odstąpienie od umowy z przyczyn leżących po stronie Zamawiającego w wysokości 20% całkowitego wynagrodzenia brutto określonego w § 4 ust. 1.

3. Strony nie odpowiadają za niewykonanie lub nienależyte wykonanie umowy będące następstwem działania siły wyższej. Dla celów niniejszej umowy określa się, że siłą wyższą jest zdarzenie nadzwyczajne, zewnętrzne i niemożliwe do zapobieżenia i przewidzenia.

4. Kary umowne powinny być zapłacone, w terminie 7 dni od daty wystąpienia przez Zamawiającego z żądaniem zapłaty. Zamawiający może potrącić należną mu kwotę kary bez zgody Wykonawcy z należności za wykonanie niniejszej umowy lub z dowolnej należności Wykonawcy.

5. Łączna wysokość kar umownych przysługujących Zamawiającemu z wszystkich tytułów od Wykonawcy nie może być wyższa niż 50% wynagrodzenia brutto określonego w §4 ust.1 umowy.

§ 7
Osoby reprezentujące Strony

Strony ustalają następujących reprezentantów przy realizacji niniejszej umowy:

1. Zamawiający: [imię i nazwisko], tel. ……, e-mail: ……
2. Wykonawca: [imię i nazwisko], tel. ……, e-mail: ……

§ 8
Zmiany umowy

1. Wszelkie zmiany niniejszej umowy wymagają zachowania formy pisemnej w postaci aneksu pod rygorem nieważności takiej zmiany.
2. Strony dopuszczają możliwość zmiany postanowień zawartej umowy w formie aneksu w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy w sytuacji, jeżeli wystąpi nieprzewidziana okoliczność o obiektywnym charakterze, która w sposób istotny wpłynie na możliwość wykonania przedmiotu umowy.

§ 9
Prawa autorskie

1. Prawa autorskie majątkowe w odniesieniu do wszystkich dokumentów (Utworu) dostarczonych przez Wykonawcę w trakcie realizacji niniejszej umowy przechodzą na Zamawiającego z chwilą ich dostarczenia Zamawiającemu.
2. Przeniesienie autorskich praw majątkowych obejmuje następujące pola eksploatacji:
   1) prawo do utrwalania i zwielokrotniania Utworu,
   2) prawo wprowadzania Utworu do pamięci komputerów i serwerów sieci komputerowych,
   3) prawo do wielokrotnego korzystania z Utworu przez Zamawiającego bez ograniczeń czasowych,
   4) prawo do rozpowszechniania Utworu przez jego publiczne udostępnianie w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym w dowolnej formie i postaci.
3. Przeniesienie autorskich praw majątkowych następuje w ramach wynagrodzenia, o którym mowa w § 4 ust. 1.

§ 10
Przetwarzanie danych osobowych

1. Zamawiający przetwarzane dane osobowe w celu realizacji i rozliczenia niniejszej umowy.
2. Na podstawie art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.U. UE. L. z 2016 r. Nr 119, s.1 ze zm.) - „dalej jako RODO" informuję, że:
   1) administratorem Pani/Pana danych osobowych jest Wójt Gminy Lipce Reymontowskie, 96-127 Lipce Reymontowskie ul. Reymonta 24;
   2) kontakt z inspektorem ochrony danych osobowych : e-mail ido@lipcereymontowskie.pl, tel. 46 831 61 97;
   3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn. „Przeprowadzenie diagnozy cyberbezpieczeństwa oraz przeprowadzenie stacjonarnego szkolenia w zakresie cyfrowego bezpieczeństwa informacji w Urzędzie Gminy Lipce Reymontowskie" znak: RGPiK.271.11.2022 prowadzonym w trybie zapytania ofertowego.
   4) odbiorcami Pani/Pana danych osobowych będą odbiorcy upoważnieni z mocy prawa w celu przeprowadzenia i kontroli niniejszego postępowania oraz osoby lub podmioty, biorcy udział w postępowaniu, którym udostępniona zostanie dokumentacja postępowania na ich wniosek, a także osoby i podmiotu upoważnione zgodnie z obowiązującymi przepisami prawa i zapisami zawartymi w niniejszym zapytaniu ofertowym,
   5) Pani/Pana dane osobowe będą przechowywane zgodnie z instrukcją kancelaryjną;
   6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego na realizację zamówienia objętego niniejszym zapytaniem ofertowym;
   7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
   8) posiada Pani/Pan:
      – na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
      – na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych*;

- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO**;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9) nie przysługuje Pani/Panu:
- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO

** Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*

*** Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.*

3. Wykonawca zobowiązuje się do spełnienia obowiązku informacyjnego z art. 14 RODO, wobec osób których dane osobowe zostaną przekazane prze z Wykonawcę w związku z realizacja niniejszej umowy.
4. Wykonawca przyjmuje do wiadomości, że przedmiot realizacji umowy jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia tj. Minister Funduszy i Polityki Regionalnej - jako Instytucja Zarządzająca POPC 2014-2020 oraz zarządzająca Centralnym Systemie Teleinformatycznym wspierającym realizację POPC 2014-2020, a także Centrum Projektów Polska Cyfrowa jako Grantodawca. W związku z powyższym w ramach badania kwalifikowalności wydatków może dojść do udostępnienia dokumentacji w tym danych osobowych tym instytucjom, które staną się wtedy Administratorem Państwa danych osobowych. Zgodnie z zapisami umowy powierzenia grantu Zamawiający został zobowiązany do spełnienia obowiązku informacyjnego przez Grantodawcę w imieniu Administratorów.
5. Mając na uwadze, że podczas wykonywania niniejszej umowy będzie dochodziło do powierzania danych osobowych, strony zawrą umowę powierzenia zgodnie z Art. 28 RODO. Wzór umowy powierzenia stanowi Załącznik nr 1 do niniejszej umowy.

§ 11
Postanowienia końcowe

1. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny.

2. Spory mogące wynikać przy realizacji niniejszej umowy będą rozstrzygane przez właściwy rzeczowo i miejscowo dla siedziby Zamawiającego sąd powszechny.

3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla Wykonawcy i dla Zamawiającego.

4. Integralną część umowy stanowią następujące załączniki:

   1) Załącznik nr 1 – Szczegółowy Opis Przedmiotu Zamówienia do Zapytania ofertowego,

   2) Załącznik nr 2 – Wzór umowy o powierzenie danych.

Zamawiający **Wykonawca**

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

na wykonanie zadania: „Przeprowadzenie diagnozy cyberbezpieczeństwa oraz przeprowadzenie stacjonarnego szkolenia w zakresie cyfrowego bezpieczeństwa informacji w Urzędzie Gminy Lipce Reymontowskie" w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00

CZĘŚĆ I
PRZEPROWADZENIE DIAGNOZY CYBERBEZPIECZEŃSTWA

1. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji w Urzędzie Gminy Lipce Reymontowskie, w tym:
   1) ocenę zgodności z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
   2) ocenę bezpieczeństwa systemów informatycznych.

2. Diagnoza cyberbezpieczeństwa w Urzędzie Gminy Lipce Reymontowskie musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. ***o krajowym systemie cyberbezpieczeństwa*** (Dz.U. z 2018 r. poz. 1560 z późn. zm.)

3. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina] - ***Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.***

4. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w ww. rozporządzeniu:
   1) Certified Internal Auditor (CIA),
   2) Certified Information System Auditor (CISA),
   3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób,
   4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób,
   5) Certified Information Security Manager (CISM),
   6) Certified in Risk and Information Systems Control (CRISC),
   7) Certified in the Governance of Enterprise IT (CGEIT),
   8) Certified Information Systems Security Professional (CISSP),
   9) Systems Security Certified Practitioner (SSCP),
   10) CertifiedReliability Professional,
   11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

5. Diagnoza cyberbezpieczeństwa musi być przeprowadzona w siedzibie Zamawiającego osobiście przez Wykonawcę, nie dopuszcza się formy zdalnej przeprowadzenia diagnozy.

6. Zamawiający nie zezwala Wykonawcy na powierzenie prac związanych z wykonaniem diagnozy cyberbezpieczeństwa osobom trzecim.

7. Wykonawca omówi wyniki przeprowadzonej diagnozy cyberbezpieczeństwa w siedzibie Zamawiającego.

8. Diagnozę cyberbezpieczeństwa należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

CZĘŚĆ II
PRZEPROWADZENIE SZKOLENIA Z ZAKRESU CYFROWEGO BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY LIPCE REYMONTOWSKIE

1. Szkolenie z zakresu cyberbezpieczeństwa ma na celu podniesienie kompetencji kadry urzędniczej w obszarze zagrożeń teleinformatycznych, podniesienie poziomu bezpieczeństwa informacyjnego w urzędzie, poznanie prawidłowej reakcji na cyberataki, poznanie podstawowych zasad i dobrych praktyk wykorzystywania technologii informatycznych oraz zdobycie umiejętności wykorzystania tej wiedzy w praktyce.

2. Informacje dotyczące jednostki, w której szkolenie ma być przeprowadzone:

1) Liczba pracowników Urzędu objętych postępowaniem – 15 osób
2) Ilość lokalizacji działalności organizacji – 1
3) Działy w organizacji: Wójt Gminy, Skarbnik Gminy, Sekretarz Gminy, Referat Finansowy, Referat Rozwoju Gospodarki Przestrzennej i Komunalnej, Wieloosobowe stanowisko pracy do spraw Organizacyjnych i Obywatelskich, Zespół Ekonomiczno-Administracyjny Oświaty.

3. Informacje dotyczące wymagań w zakresie przeprowadzenia szkolenia:

1) Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
2) Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
3) Szkolenia będą odbywać się w dni robocze w godzinach pracy Urzędu Gminy.
4) Szkolenia będą prowadzone w języku polskim.
5) Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.
6) Szkolenia prowadzone będą na podstawie zaakceptowanego prze Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
7) W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana jest przerwa trwająca 30 minut.
8) W ramach organizacji szkoleń Zamawiający zapewni:
   a) rekrutację osób biorących udział w szkoleniach,
   b) salę szkoleniową zapewniającą warunki do przeprowadzenia szkolenia,
   c) dostęp do sieci Internet.
9) W ramach organizacji szkoleń Wykonawca zapewni:
   a) materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne w formie papierowej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 1 egzemplarz materiałów szkoleniowych zostanie przekazany Zamawiającemu w celach archiwalnych,
   b) warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne przepisami bezpieczeństwa i higieny pracy,
   c) oprogramowanie oraz sprzęt komputerowy umożliwiający przeprowadzenie szkolenia,
   d) projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń,
   e) właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich,
   f) wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia,
   g) kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń,
   h) prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
      – lista obecności Uczestników szkolenia (dzienne, wypełniane oddzielnie każdego dnia szkolenia),
      – lista odbioru zaświadczeń o ukończeniu szkolenia,
      – potwierdzenie przez Uczestników odbioru materiałów szkoleniowych,
      – przeprowadzenie ankiet satysfakcji po każdym szkoleniu,

– sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

4. Ramowy zakres szkolenia:

1) Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
2) Polityka bezpieczeństwa w organizacji.
3) Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem.
4) Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony www, ataki przez telefon, phishing, spoofing, spam.
5) Bezpieczeństwo fizyczne – urządzenia, dokumenty, „czyste biurko".
6) Zabezpieczenie informatycznych nośników danych – pendrive i pamięci zewnętrzne.
7) Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
8) Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
9) Prawidłowe korzystanie z oprogramowania antywirusowego.
10) Zasady aktualizacji programów i aplikacji.
11) Szyfrowanie dokumentów i poczty elektronicznej.
12) Polityka haseł, zarządzanie dostępem i tożsamością.

5. Dodatkowe wymagania:

1) W ramach usługi zostanie przeszkolonych 15 osób w dwóch grupach.
2) Szkolenie powinno trwać minimum 4 godziny szkoleniowe dla 1 grupy szkoleniowej.

Załącznik nr 2 do umowy – Wzór umowy o powierzenie danych

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu …… w Lipcach Reymontowskich pomiędzy:
Gminą Lipce Reymontowskie z siedzibą w Lipcach Reymontowskich przy ul. Reymonta 24, 96-127 Lipce Reymontowskie, NIP 833-10-91-147, REGON 750148302
reprezentowaną przez:
Wójta Gminy Lipce Reymontowskie – Marka Sałka
zwaną w dalszej części umowy **„Administratorem”**
a
***…… prowadzącym działalność gospodarczą pod firmą …… z głównym zakładem pod adresem: ……, zamieszkałym w …… przy ul. ……, NIP: ……, REGON: ……, PESEL: ……**

***…… z siedzibą w ……, przy ul. ……, wpisaną do rejestru prowadzonego przez Sąd Rejonowy ……, …… Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: ……, NIP: ……, REGON……**
reprezentowanym przez:
……
zwanym w dalszej części umowy **„Podmiotem przetwarzającym”.**
o następującej treści:

§1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania, w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679z 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, zwanej dalej „RODO”, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

§2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane w zakresie: imię i nazwisko właściciela nieruchomości, adres właściciela nieruchomości, numer telefonu właściciela nieruchomości, numer ewidencyjny działki właściciela.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy nr …… z dnia ……. r. na zadanie pn.: „Przeprowadzenie diagnozy cyberbezpieczeństwa oraz przeprowadzenie stacjonarnego szkolenia w zakresie cyfrowego bezpieczeństwa informacji w Urzędzie Gminy Lipce Reymontowskie”.

§3
Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 lit. b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w

celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 h.

§4
Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 lit. h) RODO ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3-dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§5
Dalsze powierzenie danych do przetwarzania

1. Administrator może powierzyć Podmiotowi przetwarzającemu dane osobowe podwykonawcy do dalszego przetwarzania jedynie w celu wykonania umowy .
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na nim obowiązków ochrony danych podwykonawcy.

§6
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7
Czas obowiązywania umowy

Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas wykonania przedmiotu umowy nr …… z dnia ……. r.

§8
Rozwiązanie umowy

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
2) przetwarza dane osobowe w sposób niezgodny z umową;
3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§9
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora danych.

PODMIOT PRZETWARZAJĄCY **ADMINISTRATOR DANYCH**