UMOWA NR ……2024

(zwana dalej „Umową")

zawarta w dniu……. 2024 r. w Poniatowej,
pomiędzy:

Gmina Poniatowa
Ul. Młodzieżowa 2,
24-320 Poniatowa
NIP: 7171801288,
reprezentowaną przez:
Burmistrza -
przy kontrasygnacie Skarbnika Gminy –

zwaną/nym w dalszej części Umowy „Zamawiającym"
a
…… z siedzibą: ……., NIP: ……., REGON: ……
reprezentowaną/nym przez:
…… – (funkcja)
zwaną/ym w dalszej części Umowy „Wykonawcą",
łącznie w Umowie zwanymi „Stronami".

Niniejsza umowa jest konsekwencją przeprowadzonego postępowania, które nie wyczerpuje znamion zawartych w art. 2 ust. 1 Ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 z późn. zm.) /lub przeprowadzonego postępowania zgodnie z ustawą z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 z późn. zm.)

§ 1
Przedmiot Umowy

1. Przedmiotem umowy jest realizacja zamówienia na podstawie projektu grantowego „Cyberbezpieczny Samorząd" realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa" obejmującego pięć zadań do wykonania:
   1.1 **Zadanie 1:** Przeprowadzenie audytu wstępnego systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych w Urzędzie Miejskim w Poniatowej;
   1.2 **Zadanie 2:** Opracowanie nowych polityk i procedur oraz aktualizacja posiadanej dokumentacji w ramach opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji (dalej SZBI) w Urzędzie;
   1.3 **Zadanie 3:** Przeprowadzenie szkoleń stacjonarnych z podziałem na kadrę zarządzającą i pozostałych pracowników z zakresu bezpieczeństwa informacji dla Urzędu;

1.4 **Zadanie 4:** Przeprowadzenie szkoleń stacjonarnych z zakresu cyberbezpieczeństwa dla wszystkich pracowników Urzędu;

1.5 **Zadanie 5:** Przeprowadzenie audytu końcowego systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych w siedzibie Urzędu.

2. Ilekroć w Umowie jest mowa o „Urzędzie" strony rozumieją przez to Urząd Miejski w Poniatowej, ul. Młodzieżowa 2, 24-300 Poniatowa.

§ 2
Szczegółowy zakres usługi

1. Szczegółowy zakres **dla zadania nr 1 zamówienia:** usługi przeprowadzenia audytu wstępnego systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych obejmuje **:**

1.1 Miejscem przeprowadzenia audytu jest siedziba Urzędu.

1.2 Minimalny zakres materialny audytu wstępnego obejmuje:

1.2.1 Ocenę zgodności z normami i obowiązującymi przepisami:

a) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773)

b) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2024.1077)

c) Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych).

d) i/lub zgodność z ISO/IEC 27001

1.2.2 Ocenę poziomu bezpieczeństwa organizacyjnego związanego z posiadaną dokumentacją i procedurami.

1.2.3 Ocenę poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością.

1.2.4 Przeprowadzenie testów penetracyjnych obejmujących testy styku sieci lokalnej z Internetem, w tym analiza topologii brzegu sieci, weryfikacja mechanizmów ochronnych, próba wykrycia usług sieciowych udostępnianych do Internetu, detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet, oraz exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet.

1.2.5 Przeprowadzenie testów penetracyjnych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego, w tym analiza topologii sieci LAN, weryfikacja mechanizmów ochronnych w sieci, analiza komunikacji sieciowej, skanowanie portów TCP/UDP i próba wykrycia usług sieciowych, skanowanie hostów aktywnych w sieci, oraz exploitacja dostępnych urządzeń oraz usług w sieci LAN.

1.3 Wykonawca na podstawie przeprowadzonych czynności kontrolnych opracuje raport z audytu wstępnego.

1.4 Raporty z audytu wstępnego będzie zawierał informacje o stanie aktualnym, stwierdzonych uchybieniach oraz zalecenia pokontrolne.

1.5 Raport zostanie przekazany Zamawiającemu w formie pisemnej jak i na nośniku elektronicznym w siedzibie Urzędu.

1.6 Wyniki raportu z audytu wstępnego zostaną omówienia na spotkaniach z kadrą kierowniczą w siedzibie Urzędu.

1.7 Wykonanie części 1 przedmiotu Umowy uznaje się za zakończone po obustronnym podpisaniu protokołów przekazania, wydania i omówienia raportów z audytu wstępnego potwierdzających ich prawidłowe wykonanie.

2 Szczegółowe wymagania **dla zadania nr 2 zamówienia:** opracowania nowych polityk i procedur oraz aktualizacja posiadanej dokumentacji w ramach opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji:

2.1 Podczas opracowywania dokumentacji SZBI dla Urzędu wymagany jest podział na 4 części:

a) Polityka Bezpieczeństwa Informacji,
b) Polityka Bezpieczeństwa Danych Osobowych,
c) Polityka Bezpieczeństwa Systemów Informatycznych,
d) Polityka Bezpieczeństwa Fizycznego

2.2 Minimalny zakres materialny opracowanych polityk i procedur wchodzących w skład systemu zarządzania bezpieczeństwem informacji musi określać i obejmować:

a) Cel i zakres polityk w kontekście bezpieczeństwa informacji (BI);
b) Role i odpowiedzialności pracowników w zakresie BI;
c) Zarządzanie ryzykiem w obszarze BI;
d) Procedury zarządzania incydentami BI;
e) Deklarację stosowania zabezpieczeń;
f) Kontrole dostępu do informacji i zasobów;
g) Procedury związane z tworzeniem i prowadzeniem aktyw informacyjnych;
h) Zasady pracy na odległość i mobilny dostęp do informacji;
i) Bezpieczeństwo fizyczne pomieszczeń i obiektów związanych z BI;
j) Bezpieczeństwo fizyczne nośników informacji;
k) Bezpieczeństwo infrastruktury wspomagającej;
l) Inwentaryzacja systemów informacyjnych;
m) Zarządzanie bezpieczeństwem i ciągłością działania łańcuch dostaw;
n) Projektowanie i wdrażanie systemów teleinformatycznych;
o) Kopie zapasowe i zarządzanie ciągłością działania;
p) Sprzęt komputerowy, oprogramowanie strategiczne systemy i aplikacje;
q) Serwery, informatyczna sieć wewnętrzna;
r) Rozliczalność działań w systemach informatycznych;
s) Procedury uwzględnienia BI w procesach planowania i zarządzania ciągłością działania;
t) Procedury bezpieczeństwa informacji w relacjach z dostawcami;
u) Okresowe szkolenia i podnoszenie świadomości pracowników z zakresu BI;
v) Cykliczne audyty i monitorowanie SZBI.

2.3 Dokumentacja zostanie opracowana z uwzględnieniem przepisów:

a) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773)
b) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2024.1077)
c) Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych).
d) i/lub zgodność z ISO/IEC 27001

2.4 Dokumentacja opracowywana jest z uwzględnieniem wymagań i potrzeb stron zainteresowanych (wewnętrznych i zewnętrznych).
2.5 Dokumentacja musi zawierać opracowania uwzględniające wyniki przeprowadzonego audytu wstępnego oraz uwzględniać informacje przekazywane przez pracowników podczas spotkań projektowych.
2.6 Po opracowaniu dokumentacji, Wykonawca przekaże projekt do zatwierdzenia kierownictwu.
2.6.1 W przypadku zgłoszenia zmian lub poprawek wykonawca zobligowany jest do naniesienia poprawek lub przedstawienia pisemnych wyjaśnień w ciągu 14 dni.
2.7 Wykonawca zobligowany jest do przeglądu i aktualizacji opracowanej dokumentacji po zrealizowaniu i wdrożeniu zakupów objętych projektem Cyberbezpieczny samorząd na wezwanie Zamawiającego w terminie do 30 dni od otrzymania wezwania.
2.8 Dokumentacja zostanie przekazana przedstawicielom Urzędu w formie pisemnej jak i wersji edytowalnej na nośniku elektronicznym w siedzibie Urzędu
2.9 Wykonanie części 2 przedmiotu Umowy uznaje się za zakończone po obustronnym podpisaniu protokołów potwierdzających ich prawidłowe wykonanie po przekazaniu i wydaniu dokumentacji SZBI w siedzibie Urzędu.

3. Szczegółowe wymagania **dla zadania nr 3 zamówienia:** szkoleń z zakresu bezpieczeństwa informacji.
3.1 Szkolenia z zakresu bezpieczeństwa informacji zakładają podział na kadrę zarządzającą i szkolenia dla pozostałych pracowników.
3.2 Minimalny zakres tematyczny dla kadry zarządzającej obejmuje:
a) Omówienie obowiązujących przepisów prawa dotyczących ochrony danych i bezpieczeństwa informacji.
b) Wymagane procedury i polityki do wdrożenia oraz utrzymania systemu zarządzania bezpieczeństwem informacji.
c) Regularne przeglądy i audyty SZBI, oceny ryzyka oraz monitorowanie i raportowanie zgodności.
d) Definiowanie ról i obowiązków w kontekście zarządzania bezpieczeństwem informacji, w tym wyznaczanie odpowiedzialności za poszczególne obszary SZBI
e) Planowanie i alokacja zasobów finansowych niezbędnych do wdrożenia i utrzymania SZBI, w tym koszty technologii, szkoleń i audytów
f) Zarządzanie incydentami bezpieczeństwa
g) Zarządzanie zmianami w SZBI
h) Strategie komunikacji w organizacji dotyczące SZBI, budowanie świadomości wśród pracowników na temat znaczenia bezpieczeństwa informacji
3.3 Minimalny zakres tematyczny dla pozostałych pracowników obejmuje:
a) Wprowadzenie do bezpieczeństwa informacji;
b) Podstawowe zasady bezpieczeństwa informacji;
c) Bezpieczne praktyki w codziennej pracy;
d) Najważniejsze elementy ochrony danych osobowych;
e) Zarządzanie Dokumentami i Nośnikami Informacji;
f) Bezpieczeństwo Fizyczne;
g) Postępowanie w Przypadku Incydentu;
3.4 Celem szkoleń jest zwiększenie świadomości pracowników, zapewnienie zgodności z przepisami oraz wdrożenie nowych procedur bezpieczeństwa informacji.
3.5 Szkolenia odbywają się w formie stacjonarnej w siedzibie Urzędu.
3.6 Całkowita liczba uczestników szkoleń wynosi 50 osób.
3.7 Szkolenia muszą zakładać podział na grupy szkoleniowe, minimum 4 grupy aby uniknąć dezorganizacji normalnej pracy każdej jednostki.

3.8 Szkolenia prowadzone są w formie wykładów, warsztatów i ćwiczeń praktycznych.
3.9 Czas trwania szkolenia dla jednej grupy wynosi od 3 do 4 godzin zegarowych.
3.10 Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00-15:00.
3.11 Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń i/lub podręczników.
3.12 Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.
3.13 Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
3.14 Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia
3.15 Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.
3.16 Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.
3.17 Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
3.18 Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
3.19 Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.
3.20 Wykonanie części 3 przedmiotu Umowy uznaje się za zakończone po obustronnym podpisaniu protokołów potwierdzających ich prawidłowe wykonanie po przekazaniu i wydaniu certyfikatów ukończenia szkoleń Zamawiającemu.

4. Szczegółowe wymagania **dla zadania nr 4 zamówienia:** szkoleń z zakresu cyberbezpieczeństwa:
4.1 Celem szkoleń jest zwiększenie świadomości zagrożeń, edukowanie uczestników o aktualnych zagrożeniach cybernetycznych, takich jak phishing, ransomware, malware, ataki DDoS i inne rodzaje cyberataków. Zrozumienie, jak te zagrożenia mogą wpływać na organizację oraz jakie mogą być konsekwencje ich wystąpienia.
4.2 Minimalny zakres tematyczny szkoleń musi nawiązywać do:
a) wprowadzenia do zagadnień związanych z cyberbezpieczeństwem,
b) zarządzanie incydentami bezpieczeństwa cyfrowego,
c) ochrona przed zagrożeniami cyfrowymi,
d) bezpieczeństwo sieci i infrastruktury IT,
e) zarządzanie hasłami i uwierzytelnianiem,
f) bezpieczne korzystanie z urządzeń mobilnych ,
g) postępowanie z nośnikami danych,
h) tworzenie i zarządzanie kopiami zapasowymi,
i) ochrona logów systemowych,
j) zarządzanie bezpieczeństwem sieci,
k) przesyłanie informacji,
4.3 Całkowita liczba uczestników szkoleń wynosi 50 osób.
4.4 Szkolenia muszą zakładać podział na grupy szkoleniowe, minimum 3 grupy na każdą jednostkę aby uniknąć dezorganizacji normalnej pracy każdej jednostki.
4.5 Szkolenia prowadzone są w formie wykładów, warsztatów i ćwiczeń praktycznych.
4.6 Czas trwania szkolenia dla jednej grupy wynosi od 3 do 4 godzin zegarowych.
4.7 Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00-15:00.
4.8 Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń i/lub podręczników.
4.9 Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.
4.10 Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
4.11 Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia
4.12 Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.

4.13 Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.
4.14 Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
4.15 Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
4.16 Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.
4.17 Wykonanie części 4 przedmiotu Umowy uznaje się za zakończone po obustronnym podpisaniu protokołów potwierdzających ich prawidłowe wykonanie po przekazaniu i wydaniu certyfikatów ukończenia szkoleń Zamawiającemu.

5. Szczegółowe wymagania **dla części 5 zamówienia:** usługi przeprowadzenia audytu końcowego**:**
5.1 Miejscem przeprowadzenia audytu będzie siedziba Urzędu Gminy.
5.2 Minimalny zakres materialny audytu końcowego obejmuje:
5.3.1 Ocenę zgodności z normami i przepisami:
a) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773)
b) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2024.1077)
c) Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych).
d) i/lub zgodność z ISO/IEC 27001
5.3.2 Ocenę poziomu bezpieczeństwa organizacyjnego związanego z posiadaną dokumentacją i procedurami.
5.3.3 Ocenę poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością.
5.3.4 Przeprowadzenie testów penetracyjnych obejmujących testy styku sieci lokalnej z Internetem, w tym analiza topologii brzegu sieci, weryfikacja mechanizmów ochronnych, próba wykrycia usług sieciowych udostępnianych do Internetu, detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet, oraz exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet.
5.3.5 Przeprowadzenie testów penetracyjnych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego, w tym analiza topologii sieci LAN, weryfikacja mechanizmów ochronnych w sieci, analiza komunikacji sieciowej, skanowanie portów TCP/UDP i próba wykrycia usług sieciowych, skanowanie hostów aktywnych w sieci, oraz exploitacja dostępnych urządzeń oraz usług w sieci LAN.
5.3.6 Przeprowadzenie testów obejmujących szczegółową konfigurację zakupionych w ramach projektu grantowego urządzeń i oprogramowania zwiększającego poziom bezpieczeństwa cyfrowego
5.4 Wykonawca na podstawie przeprowadzonych czynności kontrolnych opracuje raport z audytu końcowego dla Urzędu.
5.5 Raport z audytu końcowego będzie zawierał informacje o stanie aktualnym, stwierdzonych uchybieniach oraz zalecenia pokontrolne.
5.6 Raport zostaną przekazany Zamawiającemu w formie pisemnej jak i na nośniku elektronicznym w siedzibie Urzędu.

5.7 Wyniki raportu z audytu końcowego zostaną omówione na spotkaniu z kadrą kierowniczą w siedzibie Urzędu.

5.8 Wykonanie części 5 przedmiotu Umowy uznaje się za zakończone po obustronnym podpisaniu protokołów przekazania, wydania i omówienia raportu z audytu końcowego potwierdzającego prawidłowe wykonanie.

§ 3
Obowiązki i oświadczenia Wykonawcy

1. Wykonawca zobowiązuje się do wykonania Umowy z zachowaniem zasad należytej staranności, wynikających z zawodowego charakteru prowadzonej przez siebie działalności.
2. Wykonawca zobowiązuje się, że w toku realizacji usługi używał będzie programów, materiałów, narzędzi oraz informacji, do których posiada stosowne uprawnienie i które nie naruszają praw osób trzecich, w szczególności zaś nie naruszają przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. j. Dz. U. z 2022 r., poz. 2509 ze zm.).
3. Strony ustalają, że wymiana plików będzie odbywać się za pośrednictwem dedykowanego, zabezpieczonego zasobu sieciowego (udostępnionego przez Wykonawcę). Dostęp do Zasobu będzie chroniony przy użyciu silnego szyfrowania oraz indywidualnych danych uwierzytelniających dla każdej ze Stron.

§ 4
Obowiązki i oświadczenia Zamawiającego

1. Zamawiający zobowiązuje się do zapewnienia Wykonawcy w siedzibie podmiotu audytowanego dostępu do pomieszczeń, komputerów, urządzeń oraz do systemów informatycznych niezbędnych do realizacji Umowy.
2. Zamawiający zobowiązuje się do przekazywania za pośrednictwem wyznaczonego pracownika wszelkich dokumentów lub informacji niezbędnych do prawidłowej realizacji usługi, w terminie nie dłuższym niż 1 dzień roboczy, liczonym od dnia zgłoszenia przez Wykonawcę stosownej potrzeby uzyskania informacji niezbędnych do wykonania Umowy. Przekazanie może nastąpić w dowolnej formie, nie wyłączając przesłania informacji z wykorzystaniem poczty elektronicznej lub tradycyjnej.
3. W sytuacji powstania przeszkód w wykonaniu Umowy, leżących po stronie Zamawiającego, niezwłocznie poinformuje on Wykonawcę o powyższym w formie elektronicznej pod adres email osoby, o której mowa w §10 ust. 4 pkt 1 Umowy. Okres czasowej przeszkody w wykonaniu Umowy powstały po stronie Zamawiającego powoduje przesunięcie terminu realizacji Umowy, o którym mowa w §6 ust. 1 Umowy, o ilość dni, w trakcie których Wykonawca z nie swojej winy nie mógł wykonywać Umowy w związku z trwaniem tej przeszkody.
4. Strony w toku trwania Umowy zobowiązane są do dbania o dobre imię każdego z kontrahentów, w szczególności zobowiązują się do zaniechania publicznego wyrażania opinii, poglądów, treści itp., które mogłyby naruszyć zaufanie do którejkolwiek z nich.
5. Zamawiający wyznacza pracownika, który będzie obecny przy przeprowadzaniu czynności audytowych.
6. Niezapewnienie przez Zamawiającego obecności wyznaczonego pracownika lub osoby odpowiedzialnej za obsługę informatyczną podmiotu audytowanego, o ile nie będzie to niezbędne do prawidłowej realizacji czynności audytowych, nie wstrzymuje wykonywania przez Wykonawcę obowiązków, wynikających z Umowy.

§ 5
Upoważnienie

1. W celu prawidłowego wykonywania obowiązków wynikających z niniejszej Umowy Zamawiający udziela Wykonawcy upoważnienia do przeprowadzenia wszelkich audytów i czynności zmierzających do realizacji Umowy, swoim zakresem obejmujących w szczególności: uprawnienie do przetwarzania danych, w tym danych osobowych, uprawnienie do wstępu do pomieszczeń zawierających audytowane zasoby, uprawnienie do dostępu do urządzeń, komputerów, systemów informatycznych objętych audytowaniem oraz – w przypadku zaistnienia takiej konieczności - instalacji oprogramowania informatycznego niezbędnego do realizacji Umowy, a także wykonywania wszelkich innych niezbędnych czynności faktycznych w celu realizacji obowiązków wynikających z niniejszej Umowy.

§ 6
Terminy realizacji poszczególnych części Umowy

1. Strony ustalają następujące terminy wykonania przedmiotu Umowy:
   1.1 Wykonanie części 1 przedmiotu Umowy, tj. przeprowadzenie audytu wstępnego systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych, wydaniem i omówieniem raportu z kadrą kierowniczą Urzędu ustala się do 60 dni kalendarzowych od daty podpisania niniejszej Umowy.
   1.2 Wykonanie części 2 przedmiotu Umowy, tj. opracowanie nowych polityk i procedur oraz aktualizacja posiadanej dokumentacji w ramach opracowania i wdrożenia SZBI w Urzędzie nastąpi w terminie do 60 dni kalendarzowych od dnia zakończenia części 1.
   1.3 Wykonanie części 3 przedmiotu Umowy, tj. przeprowadzenie szkoleń z podziałem na kadrę zarządzającą i pozostałych pracowników z zakresu bezpieczeństwa informacji dla nastąpi w terminie do 30 dni kalendarzowych od zakończenia części 2.
   1.4 Wykonanie części 4 przedmiotu Umowy, tj. przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla wszystkich pracowników Urzędu nastąpi w terminie do 60 dni kalendarzowych od dnia zakończenia części 3.
   1.5 Wykonanie części 5 przedmiotu Umowy, tj. przeprowadzenie audytu końcowego systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych, wydaniem i omówieniem raportu z kadrą kierowniczą Urzędu, nastąpi w terminie do 60 dni od dnia, w którym Zamawiający poinformuje Wykonawcę o zakończeniu wszystkich działań przewidzianych w ramach projektu „Cyberbezpieczny Samorząd" i wezwie Wykonawcę do realizacji części 5 przedmiotu Umowy. Wykonawca zostanie poinformowany o zakończeniu projektu nie później niż do dnia 15 marca 2026 r., celem dotrzymania terminów rozliczenia projektu przez Zamawiającego, który zgodnie z regulaminem przewidziany jest do dnia 08 maja 2026 r.

§ 7
Wynagrodzenie oraz terminy zapłaty

1. Z tytułu realizacji niniejszej Umowy Wykonawcy przysługiwać będzie wynagrodzenie (dalej „Wynagrodzenie") w kwocie …… zł netto (słownie: ……..00/100 złotych netto) powiększone o

należny podatek VAT wedle stawki obowiązującej w miesiącu wystawienia faktury VAT, płatne z dołu po zakończeniu realizacji usługi. przy czym Strony ustalają że:

1.1 wynagrodzenie za wykonanie zadania nr 1 przedmiotu Umowy tj. przeprowadzenie audytu wstępnego systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych, wydaniem i omówieniem raportu z kadrą kierowniczą Urzędu wynosi ……. zł brutto (słownie: ……złotych)

1.2 wynagrodzenie za wykonanie zadania nr 2 przedmiotu Umowy tj. opracowanie nowych polityk i procedur oraz aktualizacja posiadanej dokumentacji w ramach opracowania i wdrożenia SZBI w Urzędzie wynosi …… zł brutto (słownie: ……..…….. złotych)

1.3 wynagrodzenie za wykonanie zadania nr 3 przedmiotu Umowy tj. przeprowadzenie szkoleń z podziałem na kadrę zarządzającą i pozostałych pracowników z zakresu bezpieczeństwa informacji dla Urzędu wynosi …… zł brutto (słownie: …….. złotych)

1.4 wynagrodzenie za wykonanie zadania nr 4 przedmiotu Umowy tj. przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla wszystkich pracowników Urzędu wynosi ……..…..… zł brutto (słownie: …….. złotych)

1.5 wynagrodzenie za wykonanie zadania nr 5 przedmiotu Umowy tj. przeprowadzenie audytu końcowego systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych, wydaniem i omówieniem raportów z kadrą kierowniczą Urzędu wynosi ……..… zł brutto (słownie: ……..…….. złotych)

2. Każdorazowo podstawą wystawienia faktury za wykonaną część przedmiotu Umowy będzie fakt obustronnego podpisania protokołu stwierdzającego należyte i kompletne wykonanie danej części Umowy.
3. Zapłata wynagrodzenia nastąpi na podstawie prawidłowo wystawionej przez Wykonawcę faktury przesłanej na adres e-mail …… Zamawiającego, przelewem w terminie 14 dni od daty otrzymania faktury, na rachunek bankowy podany na fakturze.
4. Zamawiający oświadcza, że wyraża zgodę na otrzymywanie drogą elektroniczną faktury, faktury korygującej, jak również duplikatu tych faktur wystawionych przez Wykonawcę, zgodnie z powszechnie obowiązującymi przepisami, w formacie PDF, na adres e-mail: ……
5. Fakturę należy wystawić na: Gmina Poniatowa ul. Młodzieżowa 2, 24-320 Poniatowa NIP: 7171801288
6. Faktura powinna zawierać numer Umowy, na podstawie której została wystawiona.
7. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.
8. Wykonawcy nie przysługuje żadne inne dodatkowe wynagrodzenie nieprzewidziane w Umowie, ani roszczenie o zwrot kosztów poniesionych w związku z wykonaniem Umowy.
9. Faktury VAT, na których będzie figurował rachunek bankowy spoza „Białej listy", będą traktowane, jako faktury nieprawidłowe, niepodlegające zapłacie do czasu dokonania stosownych korekt. W przypadku, gdy pomiędzy wystawieniem faktury VAT, a terminem płatności Wykonawca dokona zmiany rachunku bankowego w „Białej liście" i na dzień zapłaty nie dokona on stosownej korekty, taka faktura VAT również będzie uznana za nieprawidłową, co skutkować będzie wstrzymaniem płatności. Żaden z powyższych przypadków nie stanowi opóźnienia uprawniającego Wykonawcę do odsetek ustawowych za opóźnienie lub jakichkolwiek innych.
10. Jeżeli w momencie zapłaty przez Zamawiającego numer rachunku bankowego wskazany przez Wykonawcę w fakturze VAT nie jest numerem rachunku bankowego Wykonawcy wskazanym w "Białej liście" podatników VAT, Zamawiający wstrzyma się z płatnością na rzecz Wykonawcy, bez konsekwencji wynikających z niewykonania zobowiązania lub opóźnienia w zapłacie, do momentu, w którym numer rachunku bankowego wskazany w fakturze VAT i tzw. „Białej liście" podatników VAT będą zgodne.

§ 8

Prawa autorskie

1. Wykonawcy przysługiwać będą wyłączne prawa autorskie, nieobciążone żadnymi prawami i roszczeniami osób trzecich.
2. W ramach wynagrodzenia Wykonawca:
    a) przenosi na Zamawiającego autorskie prawa majątkowe do wszystkich utworów w rozumieniu ustawy o Prawie autorskim i prawach pokrewnych, wytworzonych w trakcie realizacji przedmiotu umowy, w szczególności takich jak: Polityka Bezpieczeństwa Informacji, Polityka Bezpieczeństwa Danych Osobowych, Polityka Bezpieczeństwa Systemów Informatycznych, Polityka Bezpieczeństwa Fizycznego, Raporty z audytów wstępnych i końcowych;
    b) zezwala Zamawiającemu na korzystanie z opracowań utworów oraz ich przeróbek oraz na rozporządzanie tymi opracowaniami wraz z ich przeróbkami.
3. Zamawiający zastrzega sobie prawo dokonywania zmian w opracowaniach spowodowanych oczywistą koniecznością, bez zgody Wykonawcy.
4. Nabycie przez Zamawiającego praw, o których mowa w ust. 1, następuje z chwilą faktycznego wydania przedmiotu umowy Zamawiającemu oraz bez ograniczeń co do terytorium, czasu, liczby egzemplarzy, w zakresie następujących pól eksploatacji:
    1) użytkowania opracowań wyłącznie na własny użytek zamawiającego w celach związanych z realizacją niniejszej umowy oraz zadań Zamawiającego,
    2) zwielokrotniania opracowań dowolną techniką w dowolnej ilości,
    3) wprowadzania opracowań do pamięci komputera na dowolnej liczbie stanowisk komputerowych, do sieci multimedialnej i komputerowej,
5. Wykonawca zobowiązuje się, że wykonując umowę będzie przestrzegał przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r. poz. 2509 t.j.) i nie naruszy praw majątkowych osób trzecich, a opracowany dokument przekaże Zamawiającemu w stanie wolnym od obciążeń prawami tych osób.

§ 9

Odstąpienie od umowy

1. Odstąpienie od umowy musi nastąpić w formie pisemnej pod rygorem nieważności takiego odstąpienia i powinno zawierać uzasadnienie.
2. Zamawiającemu przysługuje prawo odstąpienia od umowy w następujących sytuacjach, w terminie 30 dni od powzięcia wiadomości o ich wystąpieniu tj.:
    a) w razie wystąpienia 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. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonanej części umowy,
    b) gdy zostanie ogłoszone zaprzestanie działalności przedsiębiorstwa Wykonawcy,
    c) gdy w ciągu 5 dni od wezwania złożonego na piśmie Wykonawca nie rozpoczął realizacji przedmiotu umowy bez uzasadnionych przyczyn albo nie kontynuuje jej w ciągu 5 dni, pomimo wezwania Zamawiającego złożonego na piśmie;
3. Wykonawca może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości, gdy Zamawiający zalega z płatnościami przekraczającymi termin płatności o dwa miesiące.
4. Odstąpienie od umowy może nastąpić za pośrednictwem listu poleconego za potwierdzeniem odbioru lub w formie pisma złożonego w siedzibie za pokwitowaniem, z chwilą otrzymania oświadczenia o odstąpieniu.

Oświadczenie zwrócone z adnotacją „nie podjęto w terminie", „adresat wyprowadził się" lub inną równoważną uznaje się za skutecznie doręczone z chwilą zwrotu korespondencji.

5. Zamawiający zapłaci Wykonawcy wynagrodzenie za przedmiot umowy wykonany do dnia odstąpienia według cen na dzień odstąpienia, pomniejszone o roszczenia Zamawiającego z tytułu kar umownych oraz ewentualne inne roszczenia odszkodowawcze.

§ 10

Kary umowne

1. W przypadku opóźnienia w wykonaniu usług, o których mowa w § 1, powstałego z przyczyn, za które odpowiedzialność ponosi Zamawiający, termin wykonania usług ulega przedłużeniu o czas trwania opóźnienia.
2. Strony postanawiają, że obowiązującą formę odszkodowania stanowić będą kary umowne w następujących przypadkach i wysokościach za:
   a) za zwłokę w wykonywaniu całości przedmiotu umowy – w wysokości 1 %, wartości wynagrodzenia umownego określonego w § 7 ust. 1 Umowy za każdy dzień zwłoki w wykonaniu przedmiotu umowy w stosunku do terminu określonego w § 6 ust. 1 Umowy.
   b) za odstąpienie od umowy przez którąkolwiek ze Stron – w wysokości 10% wartości wynagrodzenia umownego określonego w § 7 ust. 1 Umowy.
2. Jeżeli kary umowne ze wszystkich tytułów przewidzianych w umowie przekroczą 30% wynagrodzenia umownego, Zamawiający po powiadomieniu Wykonawcy może odstąpić od umowy lub żądać stosownego obniżenia wynagrodzenia.
3. Zamawiający odstępując od umowy z własnej winy, zobowiązany jest do zapłacenia Wykonawcy wynagrodzenia za wykonane zabiegi według wartości określonej protokołem wykonania usługi ustalonej przez Zamawiającego i Wykonawcę.
4. Strony zastrzegają sobie prawo dochodzenia odszkodowania uzupełniającego do wysokości rzeczywiście poniesionej szkody wraz z odsetkami. Obowiązującą formą odszkodowania za niewykonanie lub za nienależyte wykonanie umowy będzie odszkodowanie na zasadach ogólnych.
5. Zamawiający ma prawo do potrącenia należności z tytułu kary umownej z należności wynikających z faktury, o której mowa w § 7 ust. 1.
6. Wykonawca wyraża zgodę na potrącanie kar umownych z wynagrodzenia określonego w § 7 ust. 1 niniejszej Umowy.

§ 11

Zasady zachowania poufności

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

§ 12

Siła wyższa

1. W czasie trwania siły wyższej, strony Umowy zwolnione będą od wszelkiej odpowiedzialności za jej niewykonanie lub nienależyte wykonanie, jeżeli tylko okoliczności zaistnienia siły wyższej będą stanowiły przeszkodę w wykonaniu Umowy. Postanowienie ze zdania poprzedzającego zastosowanie będzie miało również w okresie bezpośrednio poprzedzającym lub następującym bezpośrednio po wystąpieniu siły wyższej, jeżeli tylko we wskazanym okresie oddziaływanie siły wyższej będzie stanowiło przeszkodę w wykonaniu Umowy.
2. Przez „siłę wyższą", o której mowa w ustępie poprzedzającym, należy rozumieć zdarzenie o charakterze przypadkowym lub naturalnym, całkowicie niezależne od woli i działania Wykonawcy lub Zamawiającego, którego nie można było przewidzieć i niemożliwe było jego zapobieżenie, w szczególności takie zdarzenia jak: powódź, włamanie, długotrwały zanik energii elektrycznej wywołany awarią dostawcy energii, zaprzestanie funkcjonowania sieci Internet, wojna, akt terroru, wprowadzenie stanu wyjątkowego etc.
3. Strona Umowy uprawniona będzie do powoływania się na siłę wyższą jednie w sytuacji, w której niezwłocznie poinformuje o powyższym drugą stronę, w sytuacji w której posiądzie przekonanie, że zdarzenie to uniemożliwia lub znacznie utrudnia wykonanie Umowy.

§ 13

Dane osobowe

1. Administratorem danych osobowych przetwarzanych w związku z realizacją Funduszy Europejskich na Rozwój Cyfrowy , w szczególności w związku z naborem 2.2 FERC jest Centrum Projektów Polska Cyfrowa (dalej jako CPPC) z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.
2. Wykonawca ma obowiązek zapoznać się oraz udostępnić do zapoznania się wszystkim osobom upoważnionym do wykonania niniejszej umowy obowiązek informacyjny, który stanowi załącznik nr 1 do niniejszej Umowy.
3. Na podstawie umowy o powierzenie grantu CPPC umocowało Zamawiającego do powierzania przetwarzania danych osobowych podmiotom wykonującym na jego zlecenie zadania związane z udzieleniem wsparcia i realizacją Projektu.
4. Jeżeli na podstawie niniejszej umowy zajdzie konieczność dalszego powierzenia przetwarzania danych osobowych i Zamawiający uzyska na to zgodę CPPC, strony zobowiązane są zawrzeć umowę dalszego powierzenia danych osobowych w rozumieniu art. 28 ust 3 RODO, zgodnie ze wzorem który stanowi załącznik nr 2 do niniejszej Umowy.

§ 14

Postanowienia końcowe

1. Strony zgodnie ustalają, że formą kontaktu wiążącą przy realizacji Umowy jest kontakt w formie pisemnej tj. kontakt listowny (na adresy korespondencyjne podane w komparycji Umowy), bądź kontakt za pośrednictwem poczty elektronicznej e-mail pod adresy osób wskazanych w ustępach poniżej – chyba że inaczej zastrzeżono w poszczególnych postanowieniach Umowy.
2. Wymiana informacji, wzajemne powiadomienia, przesyłanie dokumentacji, a także wszelkie inne ustalenia lub zgłoszenia, które winny odbywać się w trakcie obowiązywania Umowy, dokonywać się będą pomiędzy Stronami poprzez osoby upoważnione do kontaktu, o których mowa w ust. 3 i ust. 4 poniżej. Postanowienie

uregulowane w zdaniu poprzednim nie dotyczy przypadków, w których w Umowie wprost wskazano inne dane kontaktowe lub inne osoby do kontaktu w konkretnych przypadkach w niej określonych.

3. Osoby upoważnione do kontaktu ze strony Zamawiającego:
   1) ……. , tel.: ……..…, e- mail: ……...
   2) ……. , tel.: ……., e- mail: ……
4. Osoby do kontaktu ze strony Wykonawcy:
   1) ……., tel.: ……..; e- mail: ……
   2) ……., tel.: ……., e- mail: ……
5. Zmiana postanowień Umowy wymaga formy pisemnej pod rygorem nieważności.
6. Wszelkie załączniki do Umowy stanowią jej integralną część.
7. W kwestiach nieuregulowanych mają zastosowanie przepisy z Kodeksu cywilnego oraz inne przepisy powszechnie obowiązującego prawa, a także w przypadku przetwarzania danych osobowych przepisy 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) i przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781).
8. Strony ustalają, że sądem właściwym do rozstrzygania sporów mogących w przyszłości powstać na tle Umowy będzie sąd miejscowo właściwy dla siedziby Zamawiającego.
9. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

ZAMAWIAJĄCY	WYKONAWCA
_____	_____