Szudziałowo, 15 kwietnia 2022 roku

ZAPYTANIE OFERTOWE

AUDYT CYBERBEZPIECZEŃSTWA ZGODNIE Z ZAKRESEM WSKAZANYM W DOKUMENTACJI KONKURSOWEJ PROJEKTU CYFROWA GMINA

https://www.gov.pl/web/cppc/cyfrowa-gmina

Gmina Szudziałowo na podstawie zarządzenia Wójta Gminy Szudziałowo nr 2-KJ/2021 z dnia 04 stycznia 2021 roku w sprawie wprowadzenia regulaminu udzielania zamówień publicznych, których wartość nie przekracza kwoty 130 000 złotych netto, zwraca się z zapytaniem ofertowym o cenę usługi.

I. **Zamawiający**

Gmina Szudziałowo
ul. Bankowa 1
16-113 Szudziałowo
bip.ug.szudzialowo.wrotapodlasia.pl

II. Przedmiotem zadania jest przeprowadzenie **audytu cyberbezpieczeństwa w siedzibie Zamawiającego** zgodnie z **zakresem wskazanym w załączniku nr 8** do *„Regulaminu Konkursu Grantowego Cyfrowa Gmina 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 Program Operacyjny Polska Cyfrowa”.* W szczególności:

- ocena zgodności z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369);
- ocena zgodności z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 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 2017 r. poz. 2247 t.j.);
- ocena wybranych aspektów bezpieczeństwa systemów informatycznych.

Szczegółowy zakres audytu zamieszczono w załączniku nr 1 do zapytania ofertowego.

Czas trwania audytu w siedzibie Zamawiającego nie krócej niż 2 dni robocze. Zamawiający nie udostępnia dokumentacji wymaganej do przeprowadzenia audytu poza siedzibę Jednostki (audyt „na miejscu” u Zamawiającego).

III. **Do zadań Wykonawcy należeć będzie również:**

1) Przekazanie dla Zamawiającego sprawozdania z audytu cyberbezpieczeństwa opisującego kryteria dotyczące audytu, ustalenia wynikające z audytu oraz wnioski i zalecenia wypływające z audytu.

2) Przekazanie dla zamawiającego uzupełnionego załącznika numer 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina – załącznik *„Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa”.*

IV. **Audytor jest zobowiązany posiadać 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 15 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001999/O/D20181999.pdf, tj.:

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) Certified Reliability Professional

11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

Zamawiający zastrzega możliwość weryfikacji uprawnień audytora (ważność uprawnień, akredytacja jednostki wydającej uprawnienia).

V. Zamawiający wymaga, aby **Wykonawca wykazał**, że przeprowadził minimum 1 audyt w ramach programu „Cyfrowa Gmina" lub zrealizował co najmniej 3 audyty bezpieczeństwa w jednostkach administracji publicznej o podobnym zakresie w ostatnich 2 latach przed złożeniem oferty.

VI. **Kryteria i sposób oceny oferty**:

1) Przy wyborze oferty do realizacji zamawiający będzie się kierował kryterium: Cena – 100%.

2) Cenę za wykonanie zamówienia należy podać w formularzu oferty, stanowiącym załącznik nr 2 do zapytania ofertowego.

3) Cena winna obejmować wszelkie koszty niezbędne do zrealizowania zamówienia. Wykonawca sporządzając ofertę powinien przewidzieć wszelkie okoliczności mogące mieć wpływ na cenę.

VII. **Termin realizacji zamówienia**:

Wykonawca jest zobowiązany wykonać zamówienie nie później niż w terminie **4 tygodni** od dnia zawarcia umowy z Zamawiającym.

VIII. **Oferta powinna zawierać**:

1) Wypełniony **formularz ofertowy** stanowiący załącznik nr 2 do zapytania ofertowego.

2) **Dokumenty** potwierdzające wymagane **kwalifikacje** do przeprowadzenia audytu cyberbezpieczeństwa, zgodnie z pkt. IV zapytania ofertowego.

3) **Referencje** potwierdzające prawidłowe wykonanie audytu, zgodnie z pkt. V zapytania ofertowego.

IX. Miejsce i termin składania ofert:

Ofertę sporządzić należy w języku polskim w formie pisemnej na maszynie, komputerze, nieścieralnym atramentem lub długopisem. Oferta powinna być podpisana przez osobę upoważnioną. Ofertę złożyć można elektronicznie na adres: sekretariat@szudzialowo-gmina.pl do dnia **25.04.2022 r. do godziny 9:00**.

X. Termin otwarcia ofert:

25 kwietnia 2022 roku, godzina 9:10

XI. Osoba do kontaktu:

p. Renata Czaban – Tarasewicz, tel. 85 722 14 04 w. 25

XII. Załączniki:

Załącznik nr 1 – Szczegółowy zakres audytu cyberbezpieczeństwa

Załącznik nr 2 – Formularz ofertowy

Załącznik nr 3 – Istotne postanowienia umowy

WÓJT

Tadeusz Tokarewicz

Załącznik nr 1 - Szczegółowy zakres audytu

I. Ocena zgodności Jednostki z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369) dalej UoKSC.

Lp.	Opis wymagania.	Podstawa prawna.
1	Wyznaczenie osoby do kontaktu	Art. 21 UoKSC
2	Przekazanie danych osoby wyznaczonej	Art. 22 ust. 1 pkt 5 UoKSC
3	Zapewnienie zarządzania incydentem	Art. 22 ust. 1 pkt 1 UoKSC
4	Zgłaszanie incydentu	Art. 22 ust. 1 pkt 2 UoKSC Art. 23 UoKSC
5	Zapewnienie obsługi incydentu	Art. 22 ust. 1 pkt 3 UoKSC
6	Zapewnienie dostępu do wiedzy	Art. 22 ust. 1 pkt 4 UoKSC

II. Ocena wybranych aspektów bezpieczeństwa systemów informatycznych.

Lp.	Zagadnienie
1	**Dokumentacja potwierdzająca wykonane działania wskazanego w ustawie o krajowym systemie cyberbezpieczeństwa (UoKSC)**
1.1	Czy zostały zidentyfikowane usługi publiczne, których świadczenie zależy od bezpieczeństwa systemów informacyjnych?
1.2	Czy zostały wskazane osoby (podmioty) odpowiedzialne za zarządzanie incydentami?
1.3	Czy podmiot publiczny realizuje zadania publikowania informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa oraz możliwych, skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, tj. zadań zawartych w art. 22 ust. 1 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.)?
1.4	Czy została wyznaczona i zgłoszona do właściwego CSIRT, osoba kontaktowa, o której mowa w art. 21 oraz art. 22 ust. 1 pkt 5 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.)?
2	**Opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne**
2.1	Czy wszystkie elementy składowe systemu informatycznego zostały zinwentaryzowane?
2.2	Czy dla każdego systemu informatycznego utrzymywana jest aktualna lista osób odpowiedzialnych za jego bezpieczną eksploatację?
3	**Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne**
3.1	Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne?
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?
3.3	Czy istnieje dokumentacja architektury sieci?
3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?
3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?
3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?
4	**Dokumentacja procesu zarządzania incydentami**
4.1	Czy wdrożone jest monitorowanie i wykrywanie incydentów? Kto za nie odpowiada? (stanowiska, funkcje itp. - bez danych osobowych)
4.2	Czy istnieje procedura informowania o wykrytych incydentach?

4.3	Czy istnieją procedury reagowania na incydenty?
5	**Aspekty techniczne do weryfikacji**
5.1	Wyniki audytu serwisów WWW z uwzględnieniem: - wersji serwera HTTP; - wersji systemu CMS (o ile występuje); - bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.); - dostępności kompetentnego personelu do utrzymania serwisów.
5.2	Wyniki audytu serwisów pocztowych z uwzględnieniem: - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC; - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS; - dostępności kompetentnego personelu do utrzymania serwisów.
5.3	Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem: - wdrożenia systemów ochrony przed kodem szkodliwym w sposób zapewniający ich automatyczną aktualizację; - stosowania mechanizmów segmentacji sieci; - izolacji urządzeń końcowych użytkowników; - procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji; - monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa; - dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej.
5.4	Wyniki audytu połączenia z siecią Internet z uwzględnieniem: - monitorowania ruchu wchodzącego i wychodzącego; - stosowanych zabezpieczeń przed atakami DDoS; - stosowanych zabezpieczeń przed wyciekiem informacji (DLP); - stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.); - dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet.
6	**Aspekty organizacyjne do weryfikacji**
6.1	Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem: - regularnego identyfikowania znanych podatności w eksploatowanych systemach IT; - terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników; - prowadzenia okresowego przeglądu uprawnień użytkowników; - prowadzenia okresowych szkoleń użytkowników podnoszących ich świadomość zagrożeń.
6.2	Wyniki audytu procesów planowania z uwzględnieniem: - posiadania planów przywracania usług IT na wypadek awarii; - prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT; - cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta.

III. Ocena zgodności Jednostki z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 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 2017 r. poz. 2247 t.j.) dalej KRI.

Lp.	Opis wymagania	Podstawa prawna.
1	Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI
2	Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI

3	Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI
4	Aktualizowanie regulacji wewnętrznych	Par. 20 ust. 2 pkt 1 KRI
5	Inwentaryzacja sprzętu i oprogramowania	Par. 20 ust. 2 pkt 2 KRI
6	Przeprowadzanie okresowych analiz ryzyka	Par. 20 ust. 2 pkt 3 KRI
7	Postępowanie z ryzykiem	Par. 20 ust. 2 pkt 3 KRI
8	Zarządzanie uprawnieniami	Par. 20 ust. 2 pkt 4, 5 KRI
9	Szkolenia i uświadamianie	Par. 20 ust. 2 pkt 6 KRI
10	Monitorowanie dostępu do informacji	Par. 20 ust. 2 pkt 7 lit. a KRI
11	Monitorowanie nieautoryzowanych zmian	Par. 20 ust. 2 pkt 7 lit. b KRI
12	Zabezpieczenie nieautoryzowanego dostępu	Par. 20 ust. 2 pkt 7 lit. c KRI
13	Ustanowienie zasad bezpiecznej pracy mobilnej	Par. 20 ust. 2 pkt 8 KRI
14	Zabezpieczenie informacji przed nieuprawnionym ujawnieniem	Par. 20 ust. 2 pkt 9 KRI
15	Zabezpieczenie informacji przed nieuprawnioną modyfikacją	Par. 20 ust. 2 pkt 9 KRI
16	Zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem	Par. 20 ust. 2 pkt 9 KRI
17	Zawieranie w umowach serwisowych zapisów o bezpieczeństwie	Par. 20 ust. 2 pkt 10 KRI
18	Ustalenie zasad postępowania z informacjami w celu minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania	Par. 20 ust. 2 pkt 11 KRI
19	Aktualizowanie oprogramowania	Par. 20 ust. 2 pkt 12 lit. a KRI
20	Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu	Par. 20 ust. 2 pkt 12 lit. b KRI
21	Ochrona systemu przed błędami	Par. 20 ust. 2 pkt 12 lit. c KRI
22	Stosowanie mechanizmów kryptograficznych w systemach	Par. 20 ust. 2 pkt 12 lit. d KRI
23	Zapewnienie bezpieczeństwa plików systemowych	Par. 20 ust. 2 pkt 12 lit. e KRI
24	Zarządzanie podatnościami systemów	Par. 20 ust. 2 pkt 12 lit. f, g KRI
25	Kontrola zgodności systemów z regulacjami	Par. 20 ust. 2 pkt 12 lit. h KRI
26	Zapewnienie audytu bezpieczeństwa informacji, nie rzadziej niż raz na rok	Par. 20 ust. 2 pkt 14 KRI

Załącznik nr 2 – Formularz ofertowy

..... dn .....

Nazwa i siedziba Wykonawcy

.....

.....

NIP..... REGON.....

tel..... Fax.....

OFERTA WYKONAWCY

W odpowiedzi na zaproszenie do złożenia oferty z dnia 15.04.2022 r. na wykonanie zadania pn. **„Audyt cyberbezpieczeństwa w projekcie Cyfrowa Gmina"** ***w ramach działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia***, oferuję wykonanie zamówienia za łączną:

cenę **netto** audytu cyberbezpieczeństwa ..... zł plus podatek **VAT** w kwocie .....zł,

razem cena **brutto** ..... zł

słownie zł: .....

Osoba/y do kontaktu z Zamawiającym, odpowiedzialna/e za prawidłową realizację przedmiotu zamówienia:

.....

tel.....

e-mail.....

Oświadczenia:

1. Oświadczam, że zamówienie zostanie wykonane w przewidywanym przez Zamawiającego terminie, jednak nie później niż w terminie 4 tygodni od dnia zawarcia umowy.

2. Oświadczam, że zapoznaliśmy się z warunkami udziału w konkursie ofert na zamówienie dotyczące zapytania ofertowego z dnia 15.04.2022 r. ogłoszonym przez Gminę Szudziałowo, ul. Bankowa 1, 16-113 Szudziałowo, województwo podlaskie, oraz akceptujemy ich treść.

3. Oświadczam, że nie wykonywaliśmy żadnych czynności związanych z przygotowaniem niniejszego zapytania ofertowego.

4. Oświadczam, że w przypadku wyboru naszej oferty jako najkorzystniejszej, zobowiązuję się do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego.

5. Oświadczam, iż posiadamy uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień, w tym uprawnienia wskazane 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 15 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Posiadamy niezbędną wiedzę i doświadczenie konieczne do realizacji zadania. Dysponujemy odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonywania zamówienia. Znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

.....

podpis Wykonawcy

Załącznik nr 3 – Istotne postanowienia umowy

UMOWA NR .....

zawarta w dniu ..... 2022 roku w Szudziałowie,
pomiędzy
Gminą Szudziałowo z siedzibą w Szudziałowie, przy ulicy Bankowej 1, NIP: 545-17-99-806, REGON: 050659645
reprezentowaną przez:
Tadeusza Tokarewicza – Wójta Gminy Szudziałowo
zwanym dalej „**Zamawiającym**"
a
..... NIP .....
reprezentowanym przez:
.....
zwanym dalej „**Wykonawcą**"

o następującej treści:

umowa niniejsza została zawarta po przeprowadzeniu postępowania na podstawie Zarządzenia Wójta Gminy Szudziałowo nr 2-KJ/2021 z dnia 04 stycznia 2021 roku w sprawie wprowadzenia regulaminu udzielania zamówień publicznych, których wartość nie przekracza kwoty 130 000 złotych netto, dla którego nie stosuje się ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. 2021 poz. 1129) zwanej dalej ustawą.

§ 1

Przedmiot umowy

1. Przedmiotem umowy jest wykonanie zadania pn. ***„Audyt cyberbezpieczeństwa w projekcie Cyfrowa Gmina" w ramach działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia***.

2. Szczegółowy zakres zamówienia określa zapytanie ofertowe z dnia 15.04.2022 r. oraz oferta Wykonawcy z dnia ..... r. stanowiące załączniki do niniejszej umowy.

3. Wykonawca zgodnie ze złożoną ofertą, zobowiązuje się do wykonania audytu cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina" w Urzędzie Gminy Szudziałowo (w dokumentacji konkursowej projektu nazywanej „diagnozą cyberbezpieczeństwa") zgodnie z określonymi wymaganiami.

4. W zakresie zadania objętego umową obligatoryjne jest, iż Wykonawca posiada 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.

5. Wykonawcy znane są warunki realizacji przedmiotu umowy, zapoznał się z lokalizacją realizowanego zadania, założeniami i oczekiwaniami Zamawiającego co do standardu oraz jakości wykonania przedmiotu umowy.

§ 2

Termin realizacji

1. Wykonawca zobowiązuje się do wykonania przedmiotu umowy w terminie: **4 tygodni od dnia zawarcia umowy**.

§ 3
Wynagrodzenie i sposób rozliczeń

1. Za wykonanie Umowy, Wykonawcy przysługuje wynagrodzenie zgodnie ze złożoną ofertą w kwocie brutto ..... **złotych** (słownie: ..... **złotych**), w tym podatek VAT w stawce ..... % tj. ..... złotych.

2. Wynagrodzenie nie podlega waloryzacji.

3. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszystkie koszty Wykonawcy związane z realizacją przedmiotu umowy, w tym wszelkie koszty ponoszone w związku z zatrudnianiem dodatkowych osób, koszty ubezpieczenia, koszty dojazdów oraz inne koszty niezbędne do prawidłowego wykonania zadania.

4. Podstawę do wystawienia faktury stanowi prawidłowo wykonana diagnoza cyberbezpieczeństwa wraz ze złożonym przez Wykonawcę sprawozdaniem z audytu cyberbezpieczeństwa oraz wypełnionym załącznikiem nr 8 do Regulaminu Konkursu Grantowego „Cyfrowa Gmina" – załącznik *„Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa".*

5. Należność, o której mowa w ust. 1 Zamawiający wypłaci Wykonawcy przelewem na rachunek bankowy w terminie 21 dni od dnia otrzymania prawidłowo wystawionej przez Wykonawcę faktury.

6. Strony postanawiają, iż zapłata następuje w dniu obciążenia rachunku bankowego Zamawiającego.

7. W przypadku nieterminowej płatności należności Wykonawca ma prawo naliczyć Zamawiającemu odsetki ustawowe za każdy dzień zwłoki.

8. Dane do wystawienia faktury:

Nabywca: Gmina Szudziałowo, ul. Bankowa 1, 16-113 Szudziałowo, NIP: 545-17-99-806

Odbiorca: Urząd Gminy Szudziałowo, ul. Bankowa 1, 16-113 Szudziałowo

§ 4
Kary umowne

1. Strony ustanawiają odpowiedzialność za niewykonanie lub nienależyte wykonanie Umowy w formie kar umownych.

2. Wykonawca zapłaci Zamawiającemu kary umowne:

a) za zwłokę wykonania któregokolwiek z zobowiązań z przyczyn zależnych od Wykonawcy – w wysokości 0,05 % wynagrodzenia określonego w § 3 ust. 1 za każdy dzień zwłoki,

b) za zwłokę w usunięciu wad stwierdzonych przy odbiorze – w wysokości 0,5 % wynagrodzenia określonego w § 3 ust. 1 za każdy dzień zwłoki,

c) z tytułu odstąpienia od umowy z przyczyn występujących po stronie Wykonawcy w wysokości 10 % wynagrodzenia określonego w § 3 ust. 1.

§ 5
Odstąpienie od umowy

1. Zamawiający może odstąpić od Umowy w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili jej zawarcia, zawiadamiając o tym Wykonawcę na piśmie w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach.

2. W wypadku określonym w ustępie poprzedzającym postanowienia o karze umownej nie mają zastosowania.

§ 6
Postanowienia końcowe

1. Umowę uważa się za zawartą po podpisaniu jej przez obie strony – Wykonawcę i Zamawiającego.
2. W sprawach nie uregulowanych niniejszą Umową zastosowanie mają odpowiednie przepisy Kodeksu cywilnego.
3. Spory mogące wyniknąć na tle wykonania umowy rozstrzygane będą przez sąd właściwy dla siedziby Zamawiającego.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach. Jeden egzemplarz dla Wykonawcy i jeden dla Zamawiającego.

§ 7
Załączniki do Umowy

Załącznik nr 1 – Formularz ofertowy

Umowa dotyczy realizacji projektu grantowego „Cyfrowa Gmina", który jest dofinansowany w ramach „Programu Operacyjnego Polska Cyfrowa na lata 2014-2020" w ramach 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.

Wykonawca **Zamawiający**