ZAPYTANIE OFERTOWE

prowadzone zgodnie z zasadą konkurencyjności o wartości poniżej kwoty 130.000 zł na realizację zadania pn.:

„Wykonanie usług związanych z wdrożeniem SZBI wraz z dostarczeniem narzędzi do zarządzania systemem bezpieczeństwa informacji i prowadzenia analizy ryzyka i przeprowadzenie szkoleń" w ramach projektu grantowego pn. „Cyberbezpieczna Gmina Nidzica (skrót CGN)" dofinansowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027

1. Zamawiający:

Gmina Nidzica
13-100 Nidzica
ul. Plac Wolności 1
e-mail: um@nidzica.pl.

2. Szczegółowy zakres zamówienia obejmuje:

Wspólny słownik zamówień (CPV):

- Usługi doradcze w zakresie bezpieczeństwa - 79417000-0
- Usługi opracowywania oprogramowania do zarządzania systemem - 72212781-7
- Usługi opracowywania oprogramowania informatycznego - 72212517-6
- Usługi szkoleniowe - 80500000-9.

3. Opis przedmiotu zamówienia:

3.1. Przedmiotem zamówienia jest wykonanie usług związanych z wdrożeniem SZBI wraz z dostarczeniem narzędzi do zarządzania systemem bezpieczeństwa informacji i prowadzenia analizy ryzyka wraz z przeprowadzenie szkoleń w ramach projektu „Cyberbezpieczna Gmina Nidzica (skrót CGN)" dofinansowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, zgodnie z Regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd".

3.2. Do szczegółowych obowiązków Wykonawcy należeć będzie:

1. Wykonanie usług doradczych w zakresie opracowania i wdrożenia SZBI oraz przeprowadzenie analizy ryzyka obejmujące w szczególności:

1) Przegląd, aktualizację i wdrożenie dokumentacji SZBI dla 12 jednostek Gminy Nidzica;
2) Opracowanie i wdrożenie spójnych procedur do analizy ryzyka dla 12 jednostek Gminy Nidzica;

2. Wdrożenie aplikacji SaaS łącznie z usługami szkoleniowymi:

1) Udostępnienie aplikacji działającej w chmurze obliczeniowej typu SaaS służącej do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa oraz analizy ryzyka wykonanej w ramach zadań określonego w ust. 1. dla 12 jednostek Gminy Nidzica.
2) Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa wraz z testami wiedzy dla przedstawicieli kadry zarządzającej jednostek Gminy Nidzica.

3.3. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji - SZBI powinna być opracowana w oparciu o wykonane analizy, Polską Normę PN-ISO/IEC 27001, ustawę o Krajowym Systemie Cyberbezpieczeństwa, dyrektywę NIS2 i Rozporządzenie Parlamentu Europejskiego RODO, ustawę o informatyzacji podmiotów realizujących zadania publiczne oraz przepisy wykonawcze.

3.4. Minimalny zakres dokumentacji SZBI zwierające niezbędne polityki, procedury i zasady, w szczególności:

1. Polityka Bezpieczeństwa Informacji;

2. Procedura zarządzania ryzykiem;
3. Instrukcja Zarządzania Systemem Informatycznym;
4. Zasady tworzenia i zmiany haseł;
5. Zasady korzystania z systemów informatycznych;
6. Zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej;
7. Zasady korzystania z nośników danych;
8. Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
9. Procedury zarzadzania uprawnieniami;
10. Procedura niszczenia danych,
11. Procedura zarządzania zdalnym dostępem;
12. Procedura szyfrowania danych;
13. Procedury zarządzania kopiami zapasowymi;
14. Polityka czystego biurka i ekranu;
15. Procedura dostępu fizycznego do pomieszczeń;
16. Procedura postępowania z incydentami bezpieczeństwa (zgłaszanie, rejestracja, klasyfikacja i postępowanie z incydentami);
17. Zasady oceny dostawców;
18. Zasady testowania skuteczności zabezpieczeń,
19. Wykaz środków technicznych zabezpieczających sieć;
20. Wykaz środków technicznych zabezpieczających systemy infornatyczne;
21. Wykaz środków technicznych zabezpieczających punkt styku z internetem,
22. Procedury wykonywania przeglądów i konserwacji oraz zasady wycofywania sprzętu;
23. Plan ciągłości działania.

3.5. Wykonawca musi zapewnić oprogramowanie w formie usługi SaaS służące do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa i analizy ryzyka w funkcjonalności opisanej w Załączniku nr 5- Opis funkcjonalny aplikacji udostępnionej w chmurze obliczeniowej.

3.6. W ramach usług serwisowych do udostępnionego oprogramowania Wykonawca musi zapewnić usługi wsparcia świadczone do 30 czerwca 2026r:
1. Indywidualne dostosowanie systemu do potrzeb Zamawiającego (min. 20 roboczogodzin);
2. Konsultacje techniczne realizowane przez dział wsparcia (min. 20 roboczogodzin);
3. Administracja użytkownikami (min. 12 roboczogodzin);
4. Szkolenia dodatkowe (min. 10 roboczogodzin);
5. Automatyczny backup wykonywany codziennie (min. 12 roboczogodzin);
6. Aktualizacja systemu do nowych przepisów (min. 6 roboczogodzin);
7. Hosting w chmurze obliczeniowej (SaaS) (min. 5GB);
8. Bieżący serwis oprogramowania informatycznego, obejmujący usuwanie błędów i usterek.

3.7. Wymagania do prowadzenia szkoleń dla przedstawicieli kadry zarządzającej jednostek Gminy Nidzica.
1. Szkolenie będzie prowadzone dla 35 pracowników Zamawiającego pełniących funkcje kierownicze w jednostkach Gminy Nidzica.
2. Cele szkolenia:
    1) zwiększenie poziomu świadomości i wiedzy kadry kierowniczej w zakresie cyberbezpieczeństwa;
    2) zwiększenie efektywności zarządzania bezpieczeństwem informacji;
    3) skuteczne monitorowanie incydentami oraz eliminacja podatności na potencjalne zagrożenia poprzez wdrożone środki techniczne i organizacyjne.
3. Szkolenia zostaną przeprowadzone w terminach ustalonych pomiędzy stronami według zatwierdzonego przez Zamawiającego harmonogramu i programu szkoleń przy czym wszystkie szkolenia objęte przedmiotem umowy muszą się odbyć w okresie od 15 listopada 2024 roku do 15 grudnia 2024 roku.
4. Szkolenia będą się odbywały w dni robocze, w godzinach pracy Zamawiającego.
5. W uzasadnionych przypadkach program i harmonogram szkoleń może ulec zmianie.
6. Zamawiający w terminie 14 dni od dnia podpisania umowy, przedstawi do uzgodnienia upoważnionemu przedstawicielowi Wykonawcy, wstępny harmonogram i program szkoleń.

7. Wykonawca w terminie 4 dni od otrzymania wstępnego harmonogramu, o którym mowa w ust. 6 ustali z Zamawiającym ostateczny harmonogram szkoleń.
8. Jeśli wskutek ważnych niezależnych powodów szkolenie nie będzie mogło się odbyć w wyznaczonym terminie, strony wspólnie ustalą nowy termin, nie późniejszy niż 7 dni od pierwotnie ustalonej daty.

4. Wymagany termin realizacji zamówienia:

4.1. Termin opracowania, wdrożenia, przeglądu, aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji – SZBI oraz procedury identyfikacji, szacowania i tolerowania ryzyk do 15 grudnia 2024 r.

4.2. Termin przeprowadzenia szkoleń: od dnia 15.11.2024 do dnia 15.12.2024 r.

4.3. Termin udostępnienia aplikacji w chmurze obliczeniowej typu SaaS: od odbioru do dnia 30.06.2026 r.

5. Wymagania obligatoryjne stawiane Wykonawcom

Zamawiający wymaga, aby Wykonawca spełniał następujące wymagania:

5.1. Wykonawca musi w trakcie realizacji umowy zapewnić Zespół projektowy złożony min. z 6 specjalistów:
1. Kierownik zespołu projektowego
2. Audytor wew. bezpieczeństwa informacji
3. Specjalista ds. technicznych.
4. Specjalista ds. programowania,
5. Specjalista ds. wdrożenia,
6. Specjalista ds. komunikacji.

5.2. Kierownik zespołu projektowego, który będzie przeprowadzać proces audytu, musi posiadać min. doświadczenie:
1. Wiedza z zakresu prowadzenia procesu projektowego lub cyklu projektowego zatwierdzonego przez Komisję Europejską, potwierdzoną certyfikatem PRINCE2 Foundation /lub równoważnym certyfikatem potwierdzającym umiejętność prowadzenia projektu w metodologii PRINCE2.
2. Wiedza z zakresu funkcjonowania procesów bezpieczeństwa w administracji publicznej
3. Wykształcenie wyższe informatyczne,
4. Umiejętność i doświadczenie w kierowaniu zespołami w projektach zrealizowanych z udziałem środków zewnętrznych.

5.3. Audytor wew. bezpieczeństwa informacji, który będzie przeprowadzić audyt bezpieczeństwa, musi posiadać uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się poniżej:
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.

5.4. Specjalista ds. technicznych - odpowiedzialny za opracowanie i weryfikację wymagań technicznych:
1. Wykształcenie wyższe informatyczne;

2. Doświadczenie polegające na udziale jako ekspert techniczny- w okresie ostatnich 3 lat przed upływem terminu składania ofert -w co najmniej dwóch zakończonych audytach bezpieczeństwa systemów informatycznych;
3. Doświadczenie w pracy zespołowej w projektach zrealizowanych z udziałem środków zewnętrznych.

5.5. Specjalista ds. programowania - odpowiedzialny za programowanie rozwiązań chmurowych związanych z SZBI:
1. Wykształcenie wyższe informatyczne;
2. Doświadczenie polegające na udziale jako programowania aplikacji chmurowych w okresie ostatnich 3 lat przed upływem terminu składania ofert - w co najmniej 5 projektach dotyczących systemów informatycznych dedykowanych dla administracji publicznej;
3. Doświadczenie w pracy zespołowej w projektach zrealizowanych z udziałem środków zewnętrznych.

5.6. Specjalista ds. komunikacji - odpowiedzialny za zakresie koordynacji i logistyki prac zespołów projektowych:
1. Wykształcenie wyższe informatyczne;
2. Doświadczenie z okresu ostatnich 3 lat przed upływem terminu składania ofert w pracy zespołowej w projektach zrealizowanych z udziałem środków zewnętrznych.
3. Doświadczenie w zakresie koordynacji i logistyki prac zespołów projektowych i serwisowych.

5.7. Zamawiający dopuszcza łączenia funkcji maksymalnie dla 2 stanowisk, o których mowa w pkt. 5.2,5.3, 5.4. Personel wykonawcy realizujący przedmiot zamówienia musi mieć udokumentowane i potwierdzone doświadczenie i kompetencje wykazane w **Załączniku nr 4.** - Wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia.

5.8. Zamawiający wymaga, aby Wykonawca wykazał, że przeprowadził minimum 1 audyt stanu bezpieczeństwa informatycznego dla jednostek organizacyjnych administracji publicznej.

5.9. Zamawiający wymaga, aby Wykonawca wykazał, że wdrożył aplikację chmurową wspomagających zarządzanie bezpieczeństwem informacji w min. w 1 JST.

5.10. W celu potwierdzenia spełniania przez Wykonawcę warunków udziału w postępowaniu, Zamawiający żąda przedstawienia wykazu usług wykonanych w okresie ostatnich 5 latach przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, daty wykonania i podmiotów, na rzecz których usługi zostały wykonane (zgodnie z **Załącznikiem nr 3** - Wykaz zrealizowanych usług), z załączeniem dowodów określających czy te usługi zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane;

5.11. Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.

6. Kryteria oceny ofert :

Przy wyborze najkorzystniejszej oferty Zamawiający będzie kierował się następującymi kryteriami oceny:
A - CENA (podstawą wyliczeń będzie cena brutto)– 70% (max. 70 pkt.);
B - DOŚWIADCZENIE – 30% (max. 30 pkt.);

7. Opis sposobu przyznawania punktów.

7.1. Sposób oceny ofert w kryterium CENA:

Ilość punktów dla każdej oferty w tym kryterium zostanie wyliczona wg poniższego wzoru:

$$C = \frac{C\ min.}{C\ bad.} \times 70\ \%$$

1 % - 1 punkt

Gdzie:
C – ilość punktów oferty badanej
C min. – cena minimalna spośród wszystkich ofert niepodlegających odrzuceniu
C bad. – cena oferty badanej
Obliczenia dokonywane będą do dwóch miejsc po przecinku.
Maksymalnie w tym kryterium można otrzymać 70 punktów.

7.2. Sposób oceny ofert w kryterium DOŚWIADCZENIE

Doświadczenie Wykonawcy z ostatnich lat oceniane będzie zgodnie z poniższą tabelą:

Doświadczenie	Punktacja przyznana
Przeprowadzenie minimum 1 audytu stanu bezpieczeństwa informatycznego	0 pkt
Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w 1 JST	0 pkt
Przeprowadzenie minimum 3 audytów stanu bezpieczeństwa informatycznego dla jednostek organizacyjnych administracji publicznej	10 pkt
Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w 2 JST	10 pkt
Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w ponad 3 JST	20 pkt

Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w Zapytaniu ofertowym, oraz uzyska najwyższą liczbę punktów obliczoną według poniższego wzoru.
Pc = C +D

Pc – Całkowita liczba punktów uzyskanych przez badaną ofertę. C – Całkowita liczba punktów uzyskana przez badaną ofertę w kryterium „Cena ”; D – Całkowita liczba punktów uzyskana przez badaną ofertę w kryterium „Doświadczenie Wykonawcy”;
Wartość punktowa zostanie podana z dokładnością do dwóch miejsc po przecinku, a zaokrąglenie zostanie dokonane zgodnie z ogólnie przyjętymi zasadami matematyki.
W przypadku, gdy oferty Wykonawców przedstawiają taki sam bilans kryterium ceny i pozostałych kryteriów, za ofertę korzystniejszą zostanie uznana oferta Wykonawcy z zaoferowaną niższą ceną.

8. Termin składania ofert:

Ofertę należy złożyć do dnia 17.10.2024 r.
poprzez stronę internetową dla systemu Baza Konkurencyjności 2021 pod linkiem https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl, zgodnie z Instrukcją oferenta w BK2021 zamieszczoną na stronie internetowej, pod linkiem https://archiwum-bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/info/web_instruction

9. Istotne dla zamawiającego postanowienia

9.1. Wzór umowy stanowi **załącznik nr 1** do Zapytania ofertowego otwartego.

9.2. Cenę oferty należy podać w złotych polskich z dokładnością do dwóch miejsc po przecinku zgodnie z **załącznikiem nr 2** - Formularz ofertowy. Łączna cena oferty musi obejmować cały zakres zamówienia, określony w zapytaniu ofertowym.

9.3. W cenie oferty należy uwzględnić także inne koszty o ile Oferent je przewiduje (np. koszty dojazdu, opłaty, ubezpieczenia itp.). Przy obliczaniu ceny należy uwzględnić, że cena będzie obowiązywać strony przez cały okres realizacji zamówienia. Jeżeli złożono ofertę, której wybór prowadziłyby do powstania obowiązku podatkowego Zamawiającego, zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.

9.4. Ofertę jak i wszystkie składane załączniki należy podpisać bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisać potwierdzonym profilem zaufanym elektronicznej platformy usług administracji publicznej.

10. Informacje dodatkowe:

10.1. Osoba/y uprawniona/e do kontaktów: Mariusz Dobrowolski, tel. 881095707, e-mail m.dobrowolski@nidzica.pl

10.2. Postępowanie może zostać zamknięte bez dokonania wyboru, w szczególności w przypadku, gdy oferta najkorzystniejsza, przekracza kwotę jaką Zamawiający może przeznaczyć na sfinansowanie zamówienia. Postępowanie może zostać zamknięte bez wybrania którejkolwiek oferty.
10.3. Zamawiający zastrzega sobie możliwość prezentacji aplikacji do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa i analizy ryzyka.
10.4. Każdy podmiot może złożyć tylko jedna ofertę.
10.5. Nie dopuszcza się składania ofert wariantowych.
10.6. Nie dopuszcza się składania ofert częściowych.

11. Załączniki (wzory dokumentów) które mają być złożone w ramach oferty:

Załącznik nr 2 - Formularz ofertowy
Załącznik nr 3 - Wykaz wykonanych usług
Załącznik nr 4 – Wykaz osób
Załącznik nr 6 – Powiązania kapitałowe
Załącznik nr 7 – Zobowiązanie podmiotu udostępniającego zasoby

Signed by / Podpisano przez:
Jacek Kosmala
Date / Data:
2024-10-10 14:15

Załącznik nr 1 do Zapytania ofertowego

Projekt Umowy

zawarta pomiędzy:

Gminą Nidzica z siedzibą w Nidzicy przy ul. Plac Wolności 1, 13-100 Nidzica, NIP: 9840161572, REGON: 510743640 zwaną dalej **„Zamawiającym”,**
reprezentowaną przez: **……..**
przy kontrasygnacie **……..**
a

Dane wykonawcy, zwaną dalej **„Wykonawcą”**, reprezentowaną przez:

…….

W wyniku rozstrzygnięcia zapytania ofertowego prowadzonego bez zastosowania ustawy Prawo zamówień publicznych na podstawie art. 2 ust. 1 pkt 1 ustawy (wartość zamówienia poniżej kwoty 130 000 zł) oraz dokonania przez Zamawiającego wyboru oferty Wykonawcy, zawiera się umowę o następującej treści:

Przyjęte definicje

1. Aplikacja – oprogramowanie narzędziowe / informatyczne działające w modelu SaaS (Software as a Service) chronione prawem autorskim działające online za pośrednictwem strony internetowej: ……*do uzupełnienia przez wybranego Wykonawcę*……..
2. Aktualizacja – zapewnienie kolejnych wersji Aplikacji.
3. Usługa hostingowa – udostępnienie niezbędnych zasobów serwerowych i sieciowych Wykonawcy niezbędnych do sprawnego funkcjonowania Aplikacji.
4. Licencja w Modelu Subskrypcyjnym – odnosi się do uprawnień, które użytkownik Aplikacji nabywa w ramach opłaty za dostęp w ramach danej Jednostki.
5. Prawo autorskie – ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

§ 1

1. Przedmiotem zamówienia jest wykonanie usług związanych z wdrożeniem SZBI wraz z dostarczeniem narzędzi do zarządzania systemem bezpieczeństwa informacji i prowadzenia analizy ryzyka oraz przeprowadzenie szkoleń w ramach projektu grantowego pn. „Cyberbezpieczna Gmina Nidzica (skrót CGN)” dofinansowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Działania 2.2 pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”, zgodnie z Regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd”.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

2. Wszystkie usługi wykonane w ramach umowy muszą być zgodne z Opisem Przedmiotu Zamówienia określonym w zapytaniu ofertowym.
3. Zakres usług obejmuje w szczególności:
    1) Przegląd, aktualizację i wdrożenie dokumentacji SZBI dla 12 jednostek Gminy Nidzica;
    2) Opracowanie i wdrożenie spójnych procedur do analizy ryzyka dla 12 jednostek Gminy Nidzica;
    3) Udostępnienie aplikacji działającej w chmurze obliczeniowej typu SaaS służącej do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa oraz analizy ryzyka wykonanej w ramach zadań określonego w Etapie I dla 12 jednostek Gminy Nidzica.
    4) Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa wraz z testami wiedzy dla przedstawicieli kadry zarządzającej jednostek Gminy Nidzica.
4. Wykonawca musi zapewnić aplikacje w formie usługi SaaS służące do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa i analizy ryzyka w funkcjonalności zgodnej z zapytaniem ofertowym.
5. Zadaniem Wykonawcy będzie wykonywanie niezbędnych zadań i czynności w ramach umowy oraz bieżąca współpraca z Zamawiającym celem osiągnięcia zaplanowanych rezultatów usług.
6. Porozumiewanie się Zamawiającego z Wykonawcą, a także przekazywanie ustaleń, poleceń, rozwiązań, zrealizowanych zadań wynikających z ustalonych obowiązków Wykonawcy w trakcie realizacji przedmiotu zamówienia lub innych wymaganych dokumentów - następować będzie w jednej lub kilku formach, ustalonych miedzy stronami na etapie realizacji zamówienia, tj.: pisemnie, drogą elektroniczną (e-mail) lub za pomocą komunikatorów internetowych.

§ 2

Do obowiązków Wykonawcy należy w szczególności:

1. Rozstrzyganie w porozumieniu z Zamawiającym wątpliwości natury technicznej powstałych w toku wykonywania przedmiotu zamówienia.
2. Bieżące informowanie Zamawiającego o wszystkich faktach mających znaczenie dla realizacji usług, a zwłaszcza o wszystkich zagrożeniach związanych z dotrzymaniem terminu zakończenia poszczególnych usług.
3. Powołanie Zespołu projektowego.
4. Doradztwo w zakresie prowadzonych prac.
5. Współpraca z upoważnionymi pracownikami Zamawiającego w sprawach związanych z realizacją umowy.
6. Przeprowadzenie szkoleń dla przedstawicieli kadry zarządzającej jednostek Gminy Nidzica z zarządzania i oceny ryzyk bezpieczeństwem informacji, w min. 2 grupach szkoleniowych (min. 3 godz. lekcyjne każda grupa).
7. W ramach usług serwisowych do udostępnionej Aplikacji Wykonawca musi zapewnić:
    a. Indywidualne dostosowanie systemu do potrzeb Zamawiającego klienta;
    b. Konsultacje techniczne realizowane przez dział wsparcia;
    c. Administracja użytkownikami;
    d. Szkolenia dodatkowe;
    e. Automatyczny backup wykonywany codziennie,
    f. Bieżący serwis Aplikacji, obejmujący usuwanie błędów i usterek (błędy krytyczne, uniemożliwiające działanie systemu usuwane będą w terminie do 2 dni roboczych od dnia

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

zgłoszenia, pozostałe błędy usuwane będą w terminie do 10 dni roboczych od dnia zgłoszenia).

g. Aktualizacja systemu do nowych przepisów;
h. Hosting w chmurze obliczeniowej (SaaS).

§ 3

Do obowiązków Zamawiającego należy:

1. Współdziałanie z Wykonawcą w zakresie koniecznym do prawidłowej realizacji przedmiotu Umowy, w szczególności w zakresie: działań koordynacyjnych, opiniodawczych i spotkań roboczych.
2. Dostarczanie Wykonawcy niezbędnych informacji, wyjaśnień, dokumentów oraz ich kopii, wedle zgłaszanych przez niego potrzeb, w najkrótszym z możliwych terminie oraz bez zbędnej zwłoki, o ile nie są objęte prawnie klauzulą zastrzeżone i wyższą.
3. Powołanie Zespołu projektowego do koordynacji projektu.
4. Terminowa zapłata Wynagrodzenia zgodnie z postanowieniami niniejszej umowy.

§ 4

1. Wykonawca oświadcza, że dysponuje odpowiednią wiedzą, doświadczeniem oraz uprawnieniami, niezbędnymi do należytego zrealizowania przedmiotu umowy określonego w § 1 ust. 1 i zobowiązuje się wykonać zamówienie ze szczególną starannością, według najlepszej wiedzy i umiejętności, z uwzględnieniem obowiązujących przepisów prawa i przyjętych standardów, z uwzględnieniem profesjonalnego charakteru prowadzonej przez siebie działalności, wykorzystując w tym celu wszystkie posiadane możliwości, a także mając na względzie ochronę interesów Zamawiającego.
2. Wykonawca oświadcza, że dysponuje osobą odpowiedzialną za realizację i koordynację usług, która posiada stosowną wiedzę i m.in. 2 letnie doświadczenie we wnioskowanym zakresie oraz certyfikat świadczący o posiadanej wiedzy w danym zakresie.
3. Wykonawca oświadcza, że przy wykonywaniu przedmiotu umowy będzie wykorzystywał jedynie materiały, utwory, dane i informacje oraz programy komputerowe, które są zgodne z obowiązującymi przepisami prawa, a w szczególności nie naruszają dóbr osobistych, majątkowych i osobistych praw autorskich, praw pokrewnych, praw do znaków towarowych lub wzorów użytkowych bądź innych praw własności przemysłowej, a także danych osobowych osób trzecich. Gdyby doszło do takiego naruszenia wyłączną odpowiedzialność względem osób, których prawa zostały naruszone, ponosi Wykonawca.
4. Zamawiający zastrzega sobie prawo nadzorowania i wnoszenia uwag do opracowywanych dokumentów na każdym etapie ich tworzenia. W przypadku niezgodności uwag z obowiązującymi przepisami prawa, przedmiotem umowy oraz zasadami sztuki konsultingowej, Wykonawca zastrzega sobie prawo do odmowy ich wprowadzenia, po uprzednim pisemnym uzasadnieniu odmowy.

§ 5

Strony ustalają następujący sposób realizacji niniejszej umowy:

1) Dopuszcza się możliwość przekazywania materiałów za pomocą poczty elektronicznej.
2) Komunikacja Zamawiający - Wykonawca odbywa się co do zasady drogą elektroniczną za pomocą poczty elektronicznej oraz na wyznaczonych przez Zamawiającego spotkaniach projektowych (w tym spotkaniach odbiorowych).

3) Osobą koordynującą realizację wszystkich prac po stronie Zamawiającego jest: ……, tel. …… kom. ……..……..……., e-mail: ……...…… . Osoba ta posiada uprawnienia do pozyskiwania niezbędnych informacji od wszystkich jednostek organizacyjnych biorących udział w projekcie oraz kontaktowania się w z nimi bez zbędnej zwłoki i formalności.
4) Osobą koordynującą realizację wszystkich prac po stronie Wykonawcy jest: ……, tel. …… kom. ……..……..……., e-mail: ……..... . Osoba ta posiada uprawnienia do kierowania zespołem po stronie Wykonawcy oraz kontaktowania się z Zamawiającym bez zbędnej zwłoki i formalności.
5) Osobami wyznaczonymi przez Zamawiającego do odbiorów, uzgadniania i konsultacji informatycznej, merytorycznej i organizacyjnej przedmiotu umowy są:
   a) …… tel……., e-mail: ……,
   b) …… tel……., e-mail: ……,

   Zmiana osób wyznaczonych przez Zamawiającego w pkt 5 nie stanowi zmiany treści umowy i może być dokonana w czasie trwania umowy poprzez zawiadomienie Wykonawcy drogą e-mailową przez osobę koordynującą wymienioną w pkt 3.
6) Osobami do kontaktów ze strony Wykonawcy w zakresie odbiorów prac, uzgadniania spraw merytorycznych i konsultacji produktów umowy są:
   a) …… tel……., e-mail: ……..……,
   b) …… tel……., e-mail: ……..……..

§ 6

1. Wykonanie przedmiotu umowy, o którym mowa w § 1, zrealizowane zostanie przez Wykonawcę do 15.12.2024 r.
2. W ciągu 2 dni od zgłoszenia gotowości do odbioru Zamawiający przeprowadzi czynności odbiorowe. W przypadku uwag do dokumentacji Wykonawca musi dokonać stosownych korekt w terminie 2 dni od ich zgłoszenia. W przypadku braku uwag zostanie podpisany protokół odbioru usługi.

§ 7

1. Całkowite wynagrodzenie Wykonawcy za realizację przedmiotu Umowy wynosi **brutto**: **……. zł (słownie: ……. zł)** tj. …….. zł netto (słownie: ……) powiększone o 23% VAT w kwocie ……,00 zł (słownie: ……zł).
2. Podstawą do wystawiania przez Wykonawcę faktury za przedmiot umowy jest zatwierdzony przez Zamawiającego „bez zastrzeżeń” protokół odbioru usługi.
3. Wynagrodzenie będzie płatne przelewem na rachunek bankowy Wykonawcy nr …….. w terminie do 14 dni od daty otrzymania prawidłowo wystawionej faktury VAT wraz z załączoną kopią protokołu odbioru.
4. Wykonawca będzie upoważniony do wystawienia faktury na: Nabywca: Gmina Nidzica, Plac Wolności 1, 13-100 Nidzica NIP: 9840161572, Odbiorca faktury: Urząd Miejski w Nidzicy, Plac Wolności 1, 13-100 Nidzica. Wykonawca może dostarczyć fakturę do siedziby Zamawiającego osobiście, poprzez placówkę pocztową na adres: Urząd Miejski w Nidzicy, Plac Wolności 1 13-100 Nidzica lub drogą elektroniczną na adres: faktury@nidzica.pl.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

5. Za datę zapłaty przyjmuje się dzień obciążenia przez bank rachunku bankowego Zamawiającego. Termin uważa się za zachowany, jeżeli obciążenie rachunku bankowego Zamawiającego nastąpi najpóźniej w ostatnim dniu terminu płatności.
6. Zamawiający zastrzega sobie prawo rozliczania płatności wynikającej z Umowy z zastosowaniem mechanizmu podzielnej płatności, przewidzianego w przepisach ustawy o podatku od towarów i usług.
7. Wykonawca oświadcza, ze rachunek bankowy wskazany w umowie:
   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).
8. W przypadku, gdy rachunek bankowy Wykonawcy nie spełnia choćby jednego z warunków określonych w ust. 7, opóźnienie w dokonaniu płatności w terminie określonym w umowie, powstałe wskutek braku możliwości:
   a) realizacji przez Zamawiającego płatności wynagrodzenia z zastosowaniem mechanizmu podzielnej płatności i/lub
   b) 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.
9. Strony nie dopuszczają możliwości zwiększenia wynagrodzenia, o którym mowa w ust.1.
10. W razie opóźnienia w płatności Wykonawca ma prawo żądać zapłaty za opóźnienie ustawowych odsetek.

§ 8

1. Bez względu na to czy Zamawiający doznał szkody, w przypadku niewykonania lub niewłaściwego wykonania umowy Wykonawca zobowiązany jest wypłacić Zamawiającemu karę umowną:
   1) za opóźnienie w dostarczeniu przedmiotu umowy określonego w § 1 za każdy dzień zwłoki - wysokości 0,1% wartości całkowitego wynagrodzenia brutto wskazanego w § 7 ust.1,
   2) z tytułu odstąpienia od umowy z przyczyn, za które odpowiada Wykonawca - w wysokości 10% wartości całkowitego wynagrodzenia brutto wskazanego w § 7 ust.1.

2. Kary umowne należne Zamawiającemu z tytułu niniejszej umowy zostaną potrącone z wynagrodzenia Wykonawcy.

3. Jeżeli kara umowna nie może zostać potrącona zgodnie z postanowieniami ust. 2, Wykonawca wpłaci należność na rachunek bankowy Zamawiającego wskazany w nocie obciążeniowej, w terminie 14 dni od daty jej wystawienia.

4. Wykonawca oświadcza, że upoważnia Zamawiającego do potrącenia z należnego mu wynagrodzenia kar umownych naliczonych przez Zamawiającego na podstawie niniejszej umowy.

5. Zamawiający zapłaci Wykonawcy karę umowną z tytułu odstąpienia od umowy z przyczyn, za które odpowiada Zamawiający – w wysokości 10 % wartości całkowitego wynagrodzenia brutto wskazanego w § 7 ust.1.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

6. Łączna wysokość kar umownych nie może przekroczyć 20% wartości całkowitego wynagrodzenia brutto wskazanego w § 7 ust.1.

§ 9

1. Informacje dotyczące przetwarzania danych osobowych wynikające z art. 13 i 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016r., str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018r., str. 2) stanowią załączniki 1 i 2 do Umowy.
2. Wykonawca zobowiązuje się do przekazania osobom, które wyznaczył do reprezentowania Wykonawcy w związku z realizacją Umowy, treści obowiązku informacyjnego, stanowiącego załącznik nr 2 do Umowy.

§ 10

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej w postaci aneksu (numerowanego kolejnym numerem) pod rygorem nieważności, za wyjątkiem zmian zastrzeżonych w treści umowy, dla których nie jest wymagana forma pisemna w postaci aneksu.
2. Strony zobowiązują się do rozstrzygania wszelkich konfliktów na drodze polubownej, przy czym sądem właściwym do rozstrzygania spraw wynikającym z realizacji niniejszej umowy, jest sąd powszechny właściwy dla siedziby Zamawiającego.
3. W kwestiach nieuregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu Cywilnego.

§ 11

1. Wykonawca oświadcza, że jest podmiotem posiadającym majątkowe prawa autorskie uprawniające do udzielania subskrypcji licencji Aplikacji.
2. Wykonawca oświadcza, że Aplikacja udostępniona Licencjobiorcy jest wolna od wad prawnych i fizycznych oraz że jest zgodne z zaleceniami, normami i obowiązującymi wymaganiami techniczno - eksploatacyjnymi na terenie Rzeczpospolitej Polskiej.
3. Każdy Licencjobiorca uzyska dostęp do Aplikacji za pośrednictwem strony internetowej: …… .
4. Każdy pracownik Licencjobiorcy otrzyma od Wykonawcy na wskazane przez Licencjobiorcę indywidualne konto służbowe poczty elektronicznej login oraz hasło umożliwiające korzystanie z Aplikacji za pomocą sieci Internet.
5. Wykonawca udziela licencji na moduły Aplikacji wyłącznie w zakresie niezbędnym do jego używania podczas wykonywania zadań statutowych Licencjobiorców i na polach eksploatacji, które są niezbędne do prawidłowego korzystania z Aplikacji w zakresie:
    a. wykorzystania do celów służbowych wszystkich dokumentów generowanych w Aplikacji, z wyłączeniem prawa do dalszego przekazania dokumentów podmiotom trzecim,
    b. wyświetlenia dokumentów przez upoważnionych pracowników Licencjobiorcy na komputerach posiadających bezpieczny dostęp do internetu,
    c. wprowadzania i aktualizowania wszelkich danych do bazy Aplikacji przez wskazanych uprawnionych pracowników Licencjobiorcy.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

6. Licencjodawca nie ponosi odpowiedzialności za konsekwencje nieprawidłowego używania Aplikacji przez Licencjobiorcę, w tym za dane przetwarzane przez Licencjobiorcę i skutki ich przetwarzania.
7. Każdy Licencjobiorca może używać Aplikacji na służbowych komputerach stacjonarnych i przenośnych oraz służbowych urządzeniach mobilnych zgodnie z nadanymi uprawnieniami dla użytkowników.
8. Zamawiający zobowiązuje się przedsięwziąć wszelkie kroki w celu ochrony Aplikacji przed jakimkolwiek naruszeniem przysługujących Wykonawcy praw autorskich.

§12

1. Wykonawca zobowiązuje się do zachowania poufności odnośnie usług świadczonych na rzecz Zamawiającego oraz jego jednostek organizacyjnych w zakresie w jakim nie są one jawne, chyba że odrębne przepisy będą zobowiązywać do ujawnienia określonych informacji. Wykonawca może przekazywać uzyskane informacje swoim pracownikom w zakresie potrzebnym do realizacji Umowy. Przekazywanie i przechowywanie poufnych informacji i dokumentów może następować za pomocą infrastruktury teleinformatycznej Wykonawcy.
2. Informacje dotyczące wykonania przedmiotu Umowy stanowią tajemnicę przedsiębiorstwa Wykonawcy. W szczególności tajemnicę przedsiębiorstwa stanowią wszelkie informacje dotyczące metodyk prac, zasad opracowania, instrukcji, memorandów i innych dokumentów oznaczonych poprzez Wykonawcę klauzulą: „TAJEMNICA PRZEDSIĘBIORSTWA”, na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) oraz art.11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r. poz. 1233). Zamawiający zobowiązuje się do zachowania poufności odnośnie świadczenia na jego rzecz usług, a w szczególności zobowiązuje się nie udostępniać stronom trzecim tajemnicy przedsiębiorstwa Wykonawcy bez wcześniejszej zgody Wykonawcy, chyba że odrębne przepisy będą zobowiązywać do ujawnienia określonych informacji. Przekazywanie i przechowywanie poufnych informacji i dokumentów może następować za pomocą infrastruktury teleinformatycznej Zamawiającego.

§ 13

1. Wszelkie zawiadomienia oraz inna korespondencja związana z niniejsza umową wymagają zachowania formy pisemnej i powinny zostać doręczone drugiej stronie: osobiście za potwierdzeniem odbioru, przesyłką kurierską lub pocztą elektroniczną na adresy e-mail wymienione w § 5 pkt 3-6.
2. Umowa została sporządzona w formie elektronicznej i podpisana przez każdą ze Stron kwalifikowanym podpisem elektronicznym.
3. Za datę zawarcia niniejszej Umowy Strony uznają dzień złożenia kwalifikowanego podpisu elektronicznego przez ostatnią z osób podpisujących w imieniu ostatniej ze Stron.

WYKONAWCA ZAMAWIAJĄCY

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Załącznik nr 1 do umowy
nr.....
z dnia ……

Informacja dotycząca przetwarzania danych osobowych

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016r., str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018r., str. 2), zwanego dalej Rozporządzeniem, Burmistrz Nidzicy informuje, że:

1. Administratorem Pani/Pana danych osobowych jest Burmistrz Nidzicy. Siedzibą Burmistrza Nidzicy jest Urząd Miejski w Nidzicy ul. Plac Wolności 1, 13-100 Nidzica.
2. W sprawach związanych z danymi osobowymi można kontaktować się z Inspektorem ochrony danych poprzez adres e-mail: iod_gmina_nidzica@nidzica.pl lub korespondencyjnie na adres Urzędu Miejskiego w Nidzicy.
3. Pani/Pana dane osobowe będą przetwarzane w celu realizacji umowy na podstawie art. 6 ust. 1 lit. b Rozporządzenia.
4. W związku z przetwarzaniem danych w celu wskazanym powyżej, Pani/Pana dane osobowe mogą być przekazywane podmiotom realizującym zadania na rzecz administratora danych osobowych, takim jak: dostawcy oprogramowania - wyłącznie w celu zapewnienia ich sprawnego działania, operatorzy pocztowi w celu zapewnienia korespondencji, podmioty publiczne w zakresie obowiązujących przepisów prawa oraz inne podmioty, którym przekazanie Pana/Pani danych osobowych będzie niezbędne do realizacji celów przetwarzania określonych w pkt 3.
5. W szczególności na potrzeby sprawozdawczości finansowej, monitoringu, kontroli i ewaluacji w związku z realizacją projektu zgłoszonego do konkursu grantowego dane mogą być przekazane do Centrum Projektów Polska Cyfrowa z siedzibą w Warszawie (01-044), przy ul. Spokojnej 13A.
6. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji wskazanego w pkt 3 celu przetwarzania, w tym również obowiązku archiwizacyjnego wynikającego z Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
7. W związku z przetwarzaniem przez administratora danych osobowych przysługuje Pani/Panu prawo do żądania dostępu do treści danych osobowych oaz ich sprostowania, usunięcia, ograniczenia przetwarzania.
8. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych narusza przepisy Rozporządzenia.
9. Podanie przez Panią/Pana danych osobowych jest dobrowolne, ale konieczne w celu zawarcia i realizacji umowy.
10. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.

Załącznik nr 2 do umowy
nr.....
z dnia .....

Informacja przeznaczona dla osób wyznaczonych do kontaktu, których dane osobowe zostały udostępnione Gminie Nidzica w związku z realizacją umowy

Zgodnie z art. 14 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016r., str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018r., str. 2), zwanego dalej Rozporządzeniem, Burmistrz Nidzicy informuje, że:

1. Administratorem Pani/Pana danych osobowych jest Burmistrz Nidzicy. Siedzibą Burmistrza Nidzicy jest Urząd Miejski w Nidzicy ul. Plac Wolności 1, 13-100 Nidzica.
2. W sprawach związanych z danymi osobowymi można kontaktować się z Inspektorem ochrony danych poprzez adres e-mail: iod_gmina_nidzica@nidzica.pl lub korespondencyjnie na adres Urzędu Miejskiego w Nidzicy.
3. Pani/Pana dane osobowe będą przetwarzane w celu kontaktu w związku z realizacją umowy na podstawie art. 6 ust. 1 lit. b i e Rozporządzenia.
4. W związku z realizacją umowy będziemy przetwarzać takie dane jak: imię, nazwisko, numer telefonu, adres email.
5. W związku z przetwarzaniem danych w celu wskazanym powyżej, Pani/Pana dane osobowe mogą być przekazywane podmiotom realizującym zadania na rzecz administratora danych osobowych, takim jak: dostawcy oprogramowania - wyłącznie w celu zapewnienia ich sprawnego działania, operatorzy pocztowi w celu zapewnienia korespondencji, podmioty publiczne w zakresie obowiązujących przepisów prawa oraz inne podmioty, którym przekazanie Pana/Pani danych osobowych będzie niezbędne do realizacji celów przetwarzania określonych w pkt 3.
6. W szczególności na potrzeby sprawozdawczości finansowej, monitoringu, kontroli i ewaluacji w związku z realizacją projektu zgłoszonego do konkursu grantowego dane mogą być przekazane do Centrum Projektów Polska Cyfrowa z siedzibą w Warszawie (01-044), przy ul. Spokojnej 13A.
7. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji wskazanego w pkt 3 celu przetwarzania, w tym również obowiązku archiwizacyjnego wynikającego z Rozporządzenia Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych z dnia 18 stycznia 2011 r.
8. W związku z przetwarzaniem przez administratora danych osobowych przysługuje Pani/Panu prawo do żądania dostępu do treści danych osobowych oaz ich sprostowania, usunięcia, ograniczenia przetwarzania.
9. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych narusza przepisy Rozporządzenia.
10. Pani/Pana dane osobowe zostały przekazane Gminie Nidzica przez ……..
11. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.

Załącznik nr 2 do Zapytania ofertowego

FORMULARZ OFERTOWY

Nazwa wykonawcy: ……

Adres siedziby……

Tel. ……, e-mail……

NIP … ……., REGON ……

Odpowiadając na skierowane do nas zapytanie ofertowe na wykonanie przez zewnętrznych ekspertów usług wsparcia dotyczących projektu „Cyberbezpieczna Gmina Nidzica (skrót CGN)" dofinasowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, składamy ofertę następującej treści:

1. Oferujemy wykonanie zamówienia za cenę:
   Cena brutto łącznie ..... zł.
   (słownie: .....zł)
   Cena netto łącznie ..... zł.
   (słownie: .....zł)

   Na zryczałtowaną cenę łączną składają się następujące usługi:

Nazwa usługi	Wartość netto	Wartość brutto
Przegląd, aktualizację i wdrożenie dokumentacji SZBI dla 12 jednostek Gminy Nidzica;		
Opracowanie i wdrożenie spójnych procedur do analizy ryzyka dla 12 jednostek Gminy Nidzica;		
Udostępnienie aplikacji działającej w chmurze obliczeniowej typu SaaS służącej do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa oraz analizy ryzyka		
Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa wraz z testami wiedzy dla przedstawicieli kadry zarządzającej jednostek Gminy Nidzica		

2. Przyjmujemy do realizacji warunki postawione przez zamawiającego w zapytaniu ofertowym.
3. Oświadczamy, że firma jest płatnikiem podatku VAT o numerze identyfikacyjnym NIP .....
4. Oświadczam, że uważam się za związanego ofertą w terminie **30 dni** od dnia upływu terminu składania ofert.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

5. Oświadczam , że nie podlegam wykluczeniu z postępowania w związku z okolicznościami wskazanymi w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, na czas trwania tych okoliczności.
6. Wykonawca oświadcza, że posiada potencjał techniczny, osobowy, wiedzę oraz doświadczenie niezbędne do wykonania przedmiotu zamówienia.

7. Dane kontaktowe:
   Tel.: ……
   e-mail: ……...
   Osoba upoważniona do kantaku z Zamawiającym: ……..

……..., dnia ……2024 r.

.....

(podpis osoby/ osób uprawnionej /ych
do reprezentowania Wykonawcy)

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

Załącznik nr 3 do Zapytania ofertowego

WYKAZ WYKONANYCH USŁUG

Nazwa wykonawcy: ……

Adres siedziby……

Tel. ……, e-mail……

NIP … ……., REGON ……

Do wykazu należy dołączyć dokumenty potwierdzające, że usługi zostały wykonane lub są wykonywane należycie.

Lp.	Rodzaj wykonanych usług	Termin realizacji	Odbiorca usługi

……., dnia ……2024 r.

.....

(podpis osoby/ osób uprawnionej /ych do reprezentowania Wykonawcy)

Załącznik nr 4 do **Zapytania ofertowego**

Nazwa wykonawcy: ……

Adres siedziby……

Tel. ……, e-mail……

NIP … ……., REGON ……

WYKAZ OSÓB SKIEROWANYCH PRZEZ WYKONAWCĘ DO REALIZACJI ZAMÓWIENIA

Wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności.

L.p.	Imię i nazwisko	Funkcja w realizacji zamówienia	Informacja o wykształceniu, kwalifikacjach zawodowych i doświadczeniu	Podstawa dysponowania osobami[1]
1	**2**	**3**	**4**	**5**
1		**Kierownik Projektu**		*Zasób własny / oddany do dyspozycji[2] przez ……[3]*
2		**Audytor wew. bezpieczeństwa informacji**		*Zasób własny / oddany do dyspozycji przez ……*
3		**Specjalista ds. technicznych**		*Zasób własny / oddany do dyspozycji przez ……*
4		**Specjalista ds. programowania**		*Zasób własny / oddany do dyspozycji przez ……*
5		**Specjalista ds. wdrożenia**		*Zasób własny / oddany do dyspozycji przez ……*

[1] w przypadku polegania na potencjale osobowym innego podmiotu Wykonawca zobowiązany jest dołączyć, w szczególności zobowiązania innych podmiotów do oddania Wykonawcy do dyspozycji niezbędnych zasobów z zakresu zdolności technicznej lub zawodowej na potrzeby realizacji zamówienia

[2] Niewłaściwe skreślić

[3] Podać dane podmiotu, na którego zasobach polega Wykonawca

6		**Specjalista ds. komunikacji**		*Zasób własny / oddany do dyspozycji przez* ……

……., dnia ……2024 r.

.....

(podpis osoby/ osób uprawnionej /ych do reprezentowania Wykonawcy)

Załącznik nr 5. Opis funkcjonalny aplikacji udostępnionej w chmurze obliczeniowej

WYMAGANIA OGÓLNE

1. Aplikacja musi zapewniać wspomaganie elektroniczne procesów: wdrożenia, prowadzenia i aktualizacji dokumentacji SZBI oraz analizy i raportowania ryzyk bezpieczeństwa informacji w jednostkach administracji publicznej zgodnie z: §20 rozp. KRI, normą ISO 27001 oraz ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz dyrektywą NIS2.
2. Aplikacja powinna stanowić kluczowe narzędzie do monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji.
3. Aplikacja powinna zapewniać automatyzację procesu wdrożenia SZBI w jednostkach podległych JST.
4. Aplikacja powinna zapewniać redukcję kosztów związanych z bieżącym audytowaniem i wdrożeniem SZBI.
5. Aplikacja powinna zapewniać szybką wymianę danych i komunikację w zakresie incydentów bezpieczeństwa przetwarzania danych jednostek.
6. Aplikacja powinna zapewniać wsparcie procesu szkoleniowego i zapoznania z dokumentacją SZBI przez użytkowników aplikacji.
7. Aplikacja musi stanowić repozytorium centralne SZBI w szczególności: procedur obsługi incydentów, ciągłości działania oraz analizy ryzyk w jednostkach sektora publicznego zgodnie z §20 rozporządzenia Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
8. Aplikacja powinna zapewniać szybką weryfikację poprawności i spójności wdrożonej dokumentacji SZBI.
9. Aplikacja powinna zapewniać możliwość przejścia na formę elektroniczną wdrażania SZBI w jednostkach zgodnie z uzgodnionymi szablonami dokumentów na poziomie JST.

OPIS FUNKCJONALNOŚCI APLIKACJI:

1. Praca aplikacji w formie usługi SaaS (usługi w chmurze) z dowolnego urządzenia połączonego z Internetem (bez konieczności instalacji dodatkowych komponentów).
2. Odwzorowanie struktury organizacyjnej JST, w szczególności wprowadzenie jednostek i komórek organizacyjnych wraz z kontami dla pracowników oraz przydzielaniem im określonych ról i uprawnień (obsługa do 5000 kont).
3. Indywidualna konfiguracja parametrów dokumentacji SZBI poprzez uzgodnione formularze dla każdej jednostki organizacyjnej.
4. Zarządzanie bezpieczeństwem w oparciu o zdefiniowane modele procesów biznesowych.
5. Kokpit do zarządzania dokumentacją SZBI wraz z automatyczną kontrolą zgodności wdrożonej wersji dokumentu z najnowszym opublikowanym wzorcem.
6. Pełna rozliczalność wszystkich operacji wykonywanych przez użytkownika w aplikacji SZBI zgodnie z RODO i KRI.
7. Obsługa procesu udostępniania aktualnych dokumentów SZBI dla pracowników jednostek i komórek organizacyjnych.
8. Wewnętrzne forum dyskusyjne zapewniające elektroniczne konsultacje dokumentacji SZBI.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

9. Automatyczne raportowanie stanu zapoznania z poszczególnymi elementami dokumentacji SZBI w tym PBI przez uprawnionych pracowników jednostek i komórek organizacyjnych.
10. Podgląd bieżących dokumentów SZBI jednostek przez uprawnionych audytorów wewnętrznych.
11. Generowanie automatycznie redagowanych dokumentów SZBI / PBI do plików PDF.
12. Zachowanie pełnej historii zmian dokumentacji SZBI.
13. Definiowanie w aplikacji procesów biznesowych (diagram oraz opis), które pozwalają na ujednolicenie kluczowych procedur bezpieczeństwa oraz wskazanie użytkownikom zakresu czynności / odpowiedzialności.
14. Automatyczna inicjalizacja mapowania użytkowników aplikacji w procesach biznesowych zależna od określonych w Jednostce ról użytkowników.
15. Zabezpieczenie przed błędnym przypisaniem użytkownika do roli biznesowej (np. Kierownik Jednostki nie może mieć roli Inspektora Ochrony Danych).
16. Zgłaszanie incydentów i zagrożeń przez użytkowników systemu bezpośrednio do koordynatorów ze strony JST.
17. Utworzenie oraz udostępnienie planów reagowania na incydenty dla pracowników.
18. Zapewnienie zarządzania incydentami w podległych jednostkach publicznych JST przez koordynatorów.
19. Definiowanie oraz dokumentowanie działań prowadzonych po wystąpieniu incydentu/zagrożenia.
20. Prowadzenia rejestrów naruszeń bezpieczeństwa informacji i ochrony danych osobowych.
21. Prowadzenie wspólnej bazy ryzyk bezpieczeństwa informacji na poziomie JST przez uprawnione osoby odpowiedzialne za cyberbezpieczeństwo.
22. Identyfikacja i ocena ryzyk z odniesieniem do wybranych aktywów i realizowanych celów, zadań i procesów jednostek organizacyjnych zgodnie z zatwierdzoną procedurą.
23. Nadawanie priorytetów na poziomie JST dla zidentyfikowanych ryzyk oraz podejmowanie zdefiniowanych działań obniżających poziomy ryzyk przez uprawnione osoby odpowiedzialne za cyberbezpieczeństwo.
24. Prowadzenie identyfikacji i szacowania ryzyk w oparciu o wspólną bazę ryzyk zgodnie z normą ISO 27005.
25. Generowanie raportów zbiorczych wg wybranych parametrów dla zidentyfikowanych ryzyk bezpieczeństwa informacji w jednostkach JST objętych aplikacją.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Cyberbezpieczny Samorząd

Załącznik nr 6
do zapytania ofertowego
- oświadczenie o braku powiązań kapitałowych lub osobowych

Nazwa wykonawcy: ……

adres siedziby……

Tel. ……, e-mail ……

NIP ……, REGON ……

Oświadczenie Wykonawcy o braku powiązań kapitałowych lub osobowych

W związku ze złożeniem oferty na wykonanie przez zewnętrznych ekspertów usług wsparcia dotyczących projektu „Cyberbezpieczne Gmina Nidzica (skrót CGN)" dofinasowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, **oświadczam(y), że nie jestem(eśmy) powiązani z Zamawiającym osobowo lub kapitałowo.**

Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na:

- uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
- posiadaniu co najmniej 10% udziałów lub akcji,
- pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
- pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli,
- pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że może to budzić uzasadnione wątpliwości co do bezstronności tych osób.

……., dnia ……2024 r.

.....
(podpis osoby/ osób uprawnionej /ych

do reprezentowania Wykonawcy)

Załącznik nr 7 do zapytania ofertowego

Nazwa wykonawcy: ……

adres siedziby……

Tel. ……, e-mail ……

NIP ……, REGON ……

ZOBOWIĄZANIE PODMIOTU
UDOSTĘPNIAJĄCEGO ZASOBY

Ja (My) niżej podpisany (i):

……
(imię i nazwisko osoby upoważnionej do reprezentowania podmiotu udostępniającego zasoby)

działając w imieniu i na rzecz:

……
(nazwa i adres podmiotu udostępniającego zasoby)

Zobowiązuję się, do oddania nw. zasobów:

……
(określenie zasobów)

do dyspozycji Wykonawcy:

……
(nazwa i adres Wykonawcy składającego ofertę)

na potrzeby realizacji zamówienia pn.: **„Wykonanie usług związanych z wdrożeniem SZBI wraz z dostarczeniem narzędzi do zarządzania systemem bezpieczeństwa informacji i prowadzenia analizy ryzyka i przeprowadzenie szkoleń" w ramach projektu grantowego pn. „Cyberbezpieczna Gmina Nidzica (skrót CGN)" dofinansowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027**

Oświadczam, że:

a. udostępnię Wykonawcy zasoby, w następującym zakresie:
……

b. sposób wykorzystania udostępnionych przeze mnie zasobów przy wykonywaniu zamówienia publicznego będzie następujący:
……

c. zakres mojego udziału przy realizacji zamówienia publicznego będzie następujący:
……

d. okres mojego udostępnienia zasobów Wykonawcy będzie następujący:
……

……., dnia ……2024 r.

……
(podpis osoby/ osób uprawnionej /ych
do reprezentowania Wykonawcy)

Uwaga: *Niniejsze zobowiązanie wypełnia podmiot trzeci w przypadku, gdy wykonawca polega na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby w celu potwierdzenia spełniania warunków udziału w postępowaniu.*