Znak zapytania ofertowego: ZP.271.1.2.2026

ZAPYTANIE OFERTOWE

na wykonanie usługi pn.:

„Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych"

I. INFORMACJE O ZAMAWIAJĄCYM

Nazwa:	Gmina Ślemień
Adres:	ul. Krakowska 148, 34–323 Ślemień
NIP:	5531118702
tel.	+48 (33) 8654098
Adres e-mail:	sekretariat@slemien.pl

II. TRYB UDZIELENIA ZAMÓWIENIA

Niniejsze postępowanie prowadzone jest zgodnie z Art.2 ust.1 pkt.1 ustawy Prawo Zamówień Publicznych w trybie Zapytania Ofertowego, których wartość jest niższa od kwoty 170 000 zł netto oraz zgodnie z wytycznymi w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2021-2027.

III. PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest przeprowadzenie audytu bezpieczeństwa wdrożonego systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami i rekomendacjami:
   1) Rozporządzenia 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 – KRI;
   2) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – UoKSC;
   3) Narodowych Standardów Cyberbezpieczeństwa;

   oraz przeprowadzenie testów penetracyjnych systemów informatycznych zgodnie z wymaganiami określonymi w Opisie Przedmiotu Zamówienia stanowiącym załącznik nr 1 do Zapytania Ofertowego.
2. Zamawiający wymaga 24 miesięcznej gwarancji na przedmiot zamówienia.
3. Projekt finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe" Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa".
4. Wspólny Słownik Zamówień (CPV): 72800000-8 Usługi audytu komputerowego i testowania komputerów

IV. TERMIN WYKONANIA ZAMÓWIENIA

1 Termin realizacji zamówienia – **do 60 dni** od daty podpisania umowy

V. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia ubiegać się mogą wykonawcy, którzy spełniają warunki udziału w postępowaniu dotyczące wymagania w zakresie zdolności technicznej i zawodowej wykonawcy realizującego przedmiot zamówienia. Zamawiający uzna warunek za spełniony, jeżeli wykonawca wykaże, że:

1.1. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, to w tym krótszym okresie wykonał należycie minimum 2 usługi w zakresie audytu bezpieczeństwa w oparciu o KRI / UoKSC wraz z testami penetracyjnymi;

1.2. dysponuje lub będzie dysponował następującymi osobami, które skieruje do realizacji zamówienia:

1) minimum 2 osoby z uprawnieniami audytora, każda posiadająca przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, tj:

a) Certified Internal Auditor (CIA);
b) Certified Information System Auditor (CISA);
c) 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, w zakresie certyfikacji osób;
d) 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;
e) Certified Information Security Manager (CISM);
f) Certified in Risk and Information Systems Control (CRISC);
g) Certified in the Governance of Enterprise IT (CGEIT);
h) Certified Information Systems Security Professional (CISSP);
i) Systems Security Certified Practitioner (SSCP);
j) Certified Reliability Professional;
k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

2) minimum 1 osobę posiadającą przynajmniej jeden z następujących certyfikatów:

a) Certified Ethical Hacker (CEH),
b) Certified IT Security Specjalist Training (CSST)
c) Certified Penetration Testing Engineer (CPTE),
d) GIAC Exploit Researcher and Advanced Penetration Tester (GXPN),
e) Offensive Security Certified Professional (OSCP),
f) Offensive Security Certified Expert (OSCE),
g) Certified Information Security Manager (CISM),
h) Certified in Risk and Information Systems Control (CRISC),
i) Certified in the Governance of Enterprise IT (CGEIT),
j) Certified Information Systems Security Professional (CISSP),
k) Certified IT Security Specjalist (CSP)
l) Certified Information Texchnical Security Specialist (CITSS),
m) Systems Security Certified Practitioner (SSCP)
n) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

2. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy

potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.

4. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w ust. 3, potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   1) zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
   2) sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane, których wskazane zdolności dotyczą.
5. Podmiot, który zobowiązał się do udostępnienia zasobów, odpowiada solidarnie z wykonawcą, który polega na jego sytuacji finansowej lub ekonomicznej, za szkodę poniesioną przez zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów podmiot ten nie ponosi winy.

VI. PODSTAWY WYKLUCZENIA

1. Zamówienie nie może zostać udzielone podmiotowi powiązanemu osobowo lub kapitałowo z zamawiającym. 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:
   a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
   b) posiadaniu co najmniej 10 % udziałów lub akcji;
   c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
   d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej;
   e) pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że może to budzić uzasadnione wątpliwości co do bezstronności tych osób.
2. O udzielenie zamówienia ubiegać się mogą Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 roku o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

VII. WYKAZ DOKUMENTÓW STANOWIĄCYCH OFERTĘ ORAZ OŚWIADCZEŃ DOŁĄCZONYCH DO OFERTY

1 Wykaz dokumentów stanowiących ofertę:
   1) wypełniony formularz oferty – **załącznik nr 3;**
   2) oświadczenie wykonawcy – **załącznik nr 4;**
   3) aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji (kopia potwierdzona za zgodność z oryginałem przez osobę uprawnioną do reprezentowania wykonawcy);
   4) dokument określający zasady reprezentacji oraz osoby uprawnione do reprezentacji wykonawcy (jeżeli nie wynikają one z innych dokumentów załączonych przez wykonawcę do oferty), a jeżeli wykonawcę reprezentuje pełnomocnik - także pełnomocnictwo, określające zakres umocowania podpisane przez osoby uprawnione do reprezentowania wykonawcy;

5) wykaz usług, wykonanych nie wcześniej niż w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie, wraz z podaniem ich wartości, przedmiotu, daty, miejsca wykonania i podmiotów na rzecz których roboty te zostały wykonane, z załączeniem dowodów określających czy te roboty zostały wykonane należycie. Dowodami są referencje, bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – inne odpowiednie dokumenty. Wykaz musi potwierdzać spełnianie warunków udziału w postępowaniu określonych przez Zamawiającego w rozdziale V ust. 1.1 i zostać sporządzony według wzoru stanowiącego **załącznik nr 5 do Zapytania Ofertowego**

6) wykaz osób wraz z certyfikatami potwierdzającymi uprawnienia, skierowanych przez wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. Wykaz musi potwierdzać spełnianie warunków udziału w postępowaniu określonych przez Zamawiającego w rozdziale V ust. 1.2 i zostać sporządzony według wzoru stanowiącego **załącznik nr 6 do Zapytania Ofertowego.**

VIII. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
2. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych wykonawców, którzy wykonują usługi, do realizacji których te zdolności są wymagane.
3. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które usługi wykonają poszczególni wykonawcy.

IX. OPIS SPOSOBU OBLICZANIA CENY OFERTY

1 Cena oferty powinna zawierać wszelkie koszty jakie poniesie Wykonawca w celu należytego wykonania przedmiotu zamówienia z należnymi podatkami i opłatami, w tym także wszelkie koszty nie wynikające bezpośrednio z opisu przedmiotu zamówienia, opisu projektu i wzoru umowy, ale możliwe do przewidzenia przez Wykonawcę w dniu złożenia oferty.

2 Wszelkie rozliczenia związane z realizacją zamówienia dokonywane będą w walucie polskiej.

3 W Formularzu oferty należy podać cenę oferty: wartość netto i wartość brutto.

4 Prawidłowe ustalenie podatku VAT należy do obowiązków wykonawcy, zgodnie z przepisami ustawy o podatku od towarów i usług.

5 Jeżeli zaoferowana cena wydaje się rażąco niska w stosunku do przedmiotu zamówienia lub budzą wątpliwości zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w dokumentach zamówienia lub wynikającymi z odrębnych przepisów, zamawiający zażąda od wykonawcy wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny.

6 W przypadku gdy cena całkowita oferty złożonej w terminie jest niższa o co najmniej 30% od:

1) wartości zamówienia powiększonej o należny podatek od towarów i usług, ustalonej przed wszczęciem postępowania lub

2) średniej arytmetycznej cen wszystkich złożonych ofert niepodlegających odrzuceniu,

Zamawiający zwraca się o udzielenie wyjaśnień, o których mowa w ust. 5, chyba że rozbieżność wynika z okoliczności oczywistych, które nie wymagają wyjaśnienia.

7 Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na wykonawcy.

8 Odrzuceniu, jako oferta z rażąco niską ceną, podlega oferta wykonawcy, który nie udzielił wyjaśnień w wyznaczonym terminie, lub jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej w ofercie ceny.

9 Jeżeli w postępowaniu o udzielenie zamówienia, nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, zamawiający wybiera ofertę z najniższą ceną.

10 Jeżeli nie można dokonać wyboru w sposób o którym mowa w pkt 9, zamawiający wzywa wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych zawierających nową cenę.

11 W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonej oferty, w tym zaoferowanej ceny.

X. KRYTERIUM OCENY OFERT

1 Przy wyborze oferty Zamawiający będzie kierować się następującymi kryteriami i ich znaczeniami:

Lp.	Kryteria	Waga
1.	Cena (C)	100%

2 Punkty przyznawane za podane w pkt. X kryterium „Cena – „C" będą liczone według następującego wzoru:

$$C = \frac{C_{min}}{C_{bad}} \; x \; 100 \; x \; 100\%$$

gdzie:

C_{min} – najniższa zaoferowana cena oferty
C_{bad} – cena oferty badanej

XI. KOMUNIKACJA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCAMI

1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między Zamawiającym a Wykonawcą, odbywa się przy użyciu środków komunikacji elektronicznej.
2. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia lub znakiem sprawy (numer referencyjny postępowania).
3. Komunikacja ustna dopuszczalna jest w odniesieniu do informacji, które nie są istotne, w szczególności nie dotyczą ogłoszenia o zamówieniu lub dokumentów zamówienia, potwierdzenia zainteresowania, ofert, o ile jej treść jest udokumentowana.
4. Osobami uprawnionymi do kontaktu z Wykonawcami są:
   1) w zakresie procedury przetargowej:

      Tomasz Józefiak -tel. 33 865 40 98 wew. 33,

2) w zakresie przedmiotu zamówienia:

Krzysztof Gumula –tel. 501 830 622

5. Środkami komunikacji elektronicznej w postępowaniu o udzielenie zamówienia jest poczta elektroniczna przesyłana na adres skrzynki e-mail: sekretariat@slemien.pl
6. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim.
7. Oferty, oświadczenia, podmiotowe środki dowodowe, zobowiązanie podmiotu udostępniającego zasoby, pełnomocnictwa, sporządza się w postaci elektronicznej.
8. Dokumenty elektroniczne przekazuje się w postępowaniu przy użyciu środków komunikacji elektronicznej wskazanych w ust. 5.
9. W sprawach nieuregulowanych w niniejszym Rozdziale zastosowanie mają przepisy rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r. poz. 2452).

XII. TERMIN SKŁADANIA OFERT

1. Oferty należy składać do dnia **26 stycznia 2026 roku do godz. 11:00** w sekretariacie Urzędu Gminy w Ślemieniu, ul. Krakowska 148, 34-323 Ślemień z dopiskiem „Oferta - **Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych"** lub przesłać drogą elektroniczną na adres pocztowy e-mail: sekretariat@slemien.pl jako dokument/dokumenty elektronicznie podpisane kwalifikowanym podpisem elektronicznym, profilem zaufanym lub podpisem osobistym.
2. Oferty złożone po terminie nie będą rozpatrywane.

XIII. PRZESŁANKI ODRZUCENIA OFERT:

1. Zamawiający odrzuci ofertę, jeżeli:
   1) została złożona po terminie składania ofert;
   2) jeżeli została złożona przez Wykonawcę, który nie złożył dokumentów, o których mowa w Dziale VI;
   3) jej treść jest niezgodna z warunkami zamówienia;
   4) została złożona w warunkach czynu nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
   5) zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia;
   6) zawiera błędy w obliczeniu ceny;

XIV. PRZESŁANKI UNIEWAŻNIENIA POSTĘPOWANIA

1. Zamawiający unieważni postępowanie, jeżeli:
   1) nie złożono żadnej oferty;
   2) wszystkie złożone oferty podlegały odrzuceniu;
   3) cena najkorzystniejszej oferty przewyższa kwotę, jaką Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty.

XV. OCHRONA 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) RODO, informujemy, że:

1) administratorem Pani/Pana danych osobowych jest - **Wójt Gminy Ślemień, ul. Krakowska 148, 34-323 Ślemień, tel. +48 (033) 865 40 98;**
2) dane kontaktowe do Inspektora Ochrony Danych: Urząd Gminy w Ślemieniu, ul. Krakowska 148, 34-323 Ślemień, tel. (033) 865 40 98, mail: iod@slemien.pl ;
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego w trybie zapytania ofertowego pod nazwą: **„Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych"** – nr referencyjny ZP.271.1.2.2026;
4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania;
5) Pani/Pana dane osobowe będą przechowywane, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
6) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
7) posiada Pani/Pan:
   a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy oraz nie może naruszać integralności protokołu oraz jego załączników);
   c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
   d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa), gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
8) nie przysługuje Pani/Panu:
   a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

XVI. ZAŁĄCZNIKI

1. Załącznikami do zaproszenia są:
   1) Opis Przedmiotu Zamówienia – załącznik nr 1
   2) wzór umowy – załącznik nr 2
   3) formularz ofertowy – załącznik nr 3
   4) oświadczenie wykonawcy – załącznik nr 4
   5) wykaz usług – załącznik nr 5
   6) wykaz osób – załącznik nr 6
   7) Klauzula informacyjna FERC

WÓJT
Jarosław Krzak

Załącznik nr 1 do Zapytania Ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego w trybie Zapytania Ofertowego, pod nazwą:

Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych

realizowanego w ramach projektu

Cyberbezpieczny urząd Gminy Ślemień

Zamawiający: Gmina Ślemień, ul. Krakowska 148, 34–323 Ślemień

Projekt finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe" Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa"

I. Wymagania dotyczące Audytu bezpieczeństwa i Testów penetracyjnych

1. Audyt bezpieczeństwa musi być zgodny z wymaganiami Ustawy z dnia 13 sierpnia 2018 roku o Krajowym Systemie Cyberbezpieczeństwa, 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, rekomendacjami NSC oraz z aktualnymi wymaganiami normy PN-EN ISO IEC 27001.
2. W ramach wykonywania testów penetracyjnych aplikacji wymagane jest wykorzystanie obowiązujących standardów bezpieczeństwa udostępnianych przez organizację OWASP (Open Web Application Security Project) lub równoważnych.
3. Testy penetracyjne powinny być wykonane zgodnie ze standardami określonymi przez:
   1) OWASP Application Security Verification Standard (ASVS) w wersji 4.0.1 lub 4.0.2 https://owasp.org/www-project-application-security-verification-standard/
   2) OWASP Web Security Testing Guide (WSTG) w wersji 4.2 https://owasp.org/www-project-web-security-testing-guide/v42/
   3) Penetration Testing Execution Standard (PTES)
4. Proces testowania musi zapewnić, że każdorazowe badanie z uwzględnieniem metodyki zawartej w normach branżowych, będzie składało się z następujących, wyróżnionych etapów:
   1) przeprowadzenie badań i testów;
   2) opracowanie oceny eksperckiej;
   3) przedstawienie wiążącego stanowiska;
   4) przedstawienie rekomendacji zmian.
5. Zakres audytu bezpieczeństwa i testów penetracyjnych
   1) Audyt konfiguracji systemów operacyjnych, obejmujący sprawdzenie:
      a) uruchomionych usług sieciowych,
      b) kont systemowych,
      c) mechanizmów uwierzytelniania i autoryzacji,
      d) wdrożonych mechanizmów dostępu do zasobów,
      e) uprawnień do zasobów,
      f) wdrożonych mechanizmów instalacji aktualizacji,
      g) wdrożonych mechanizmów tworzenia kopii zapasowych,
      h) wdrożonych mechanizmów logowania zdarzeń,
      i) wdrożonych mechanizmów administracji zdalnej,
      j) wdrożonych mechanizmów zabezpieczenia systemu w fazie boot,
      k) wdrożonych mechanizmów zarządzania systemem,
      l) wdrożonych dodatkowych metod ochrony,
   2) Audyt konfiguracji baz danych, obejmujący:
      a) sprawdzenie wdrożenia podstawowych zasad hardeningowych bazy (np.: dostępność domyślnych użytkowników guest, partycjonowanie bazy, składowanie logów, logowanie nietypowych zdarzeń, dostępność wybranych niebezpiecznych procedur /funkcji składowanych);

b) sprawdzenie komunikacji z klientem bazodanowym - wykorzystanie mechanizmów kryptograficznych (logowanie się klienta oraz transfer danych);

c) ogólną recenzję architektury bazy (wykorzystane mechanizmy autoryzacji oraz uwierzytelniania segmentacja uprawnień, wykorzystanie widoków; wykorzystanie procedur składowanych);

d) weryfikację sposobu wykonywania kopii zapasowych oraz ich odtwarzania;

e) analizę sposobu udostępnienia zarządzania bazą danych na poziomie sieciowym.

3) Audyt bezpieczeństwa aplikacji, obejmujący

a) sprawdzenie architektury sieciowej i serwerowej; pod kątem bezpieczeństwa;

b) sprawdzenie procedur zarządzania serwerami;

c) sprawdzenie podatności komponentów aplikacji (w tym serwerów aplikacyjnych i baz danych);

d) weryfikację sposobu instalacji aplikacji i procedur stosowanych przy wdrażaniu nowych aplikacji;

e) weryfikację mechanizmów uwierzytelniania / autoryzacji;

f) Przeprowadzenie testów szczegółowych:

- sprawdzenie zabezpieczeń panelu administracyjnego przed nieupoważnionym dostępem,
- próba uzyskania dostępu do panelu administracyjnego za pomocą kont zwykłych użytkowników min. przez: wykorzystanie bieżącej sesji, podniesienie uprawnień,
- próba uzyskania większych uprawnień,
- próba uzyskania nieautoryzowanego dostępu do danych znajdujących się w systemie,
- próba uzyskania nieautoryzowanego dostępu do plików znajdujących się na serwerze,
- analiza możliwości enumeracji użytkowników,
- próba ataków typowych dla aplikacji webowych i web services, m.in.: SQL Injection, Cross Site Scripting, IMAP/SMTP Injection, LDAP Injection, ORM Injection, XML Injection, XPath Injection, Code Injection, Command Injection, HTTP Splitting,
- funkcja przekierowujących pod kątem walidacji wprowadzanych danych,
- analiza polityki haseł w aplikacji,
- próba ominięcia mechanizmu uwierzytelniania za pomocą min. analizy identyfikatorów sesji, manipulacji parametrami, bezpośredniego dostępu do widoku aplikacji,
- próba ominięcia mechanizmu autoryzacji min. przez uzyskanie bezpośredniego dostępu do zasobów, manipulacje parametrami, uzyskanie wyższych uprawnień,
- analiza wykorzystywanego przez aplikację szyfrowania przesyłanych danych, pod kątem dostępnych/wykorzystywanych algorytmów,
- analiza mechanizmu logowania pod kątem możliwości ominięcia uwierzytelniania i możliwości podsłuchu przesyłanych danych,
- analiza mechanizmu zakończenia sesji użytkownika pod kątem skuteczności i możliwości przeprowadzenia ataku Denial of Service,
- analiza zabezpieczenia plików Cookie,
- analiza zabezpieczenia serwera przed niebezpiecznymi metodami http,
- analiza przesyłanego kodu pod kątem zawartości zbędnych informacji o aplikacji,
- analiza nagłówków http pod kątem bezpieczeństwa,
- analiza błędów aplikacji pod kątem ujawniania informacji,
- analiza możliwości zapamiętywania przez przeglądarkę informacji klientów,
- próba odnalezienia wcześniejszych wersji kodu źródłowego i plików kopii zapasowych na serwerze.

4) Audyt bezpieczeństwa infrastruktury, obejmujący:

a) audyt architektury bezpieczeństwa infrastruktury IT;

b) audyt konfiguracji urządzeń sieciowych

c) testy penetracyjne zewnętrzne:
   - identyfikacje dostępnych serwisów sieciowych, określenie oraz weryfikacja ich podatności;
   - penetracja systemu za pomocą skanerów TCP i UDP;
   - bezpieczeństwo aplikacji oraz usług dostępnych z zewnątrz;
   - analiza topologii sieci widzianej z zewnątrz;
   - możliwość uzyskania nieautoryzowanego dostępu do danych;
   - badanie podatności związanych atakami typu DDoS;
   - konfiguracja komunikacji z usługami (np. konfiguracja SSL/TSL, IPsec);
   - weryfikacja procedur zarządzania siecią WAN.

d) testy penetracyjne wewnętrzne:
   - bezpieczeństwo urządzeń sieciowych;
   - bezpieczeństwo protokołów trasowania;
   - analiza topologii sieci i logiki jej segmentacji;
   - bezpieczeństwo maszyn zlokalizowanych w obrębie sieci (serwery, stacje robocze);
   - bezpieczeństwo usług zlokalizowanych na każdym z dostępnych w sieci urządzeniu oraz maszynie, Istnienie nieautoryzowanych urządzeń (np. nieautoryzowanego urządzenia bezprzewodowego wpiętego do sieci);
   - filtrowanie komunikacji wewnętrznej (np. konfiguracja firewall, IDS/IPS, WAF, separacja pomiędzy kluczowymi podsieciami);
   - konfiguracja komunikacji z zasobami (np. konfiguracja SSL/TLS dla kluczowych aplikacji);
   - możliwość uzyskania nieautoryzowanego dostępu do danych (np. danych wrażliwych);
   - przegląd danych dostępnych na udziałach sieciowych – weryfikujemy, czy możliwe jest uzyskanie nieautoryzowanego dostępu do danych na udziałach sieciowych takich jak hasła do systemów, czy też kluczowych dla działania organizacji danych;
   - podatność na ataki DDoS;
   - weryfikacja zasad bezpieczeństwa na wybranych stacjach roboczych;
   - weryfikacja dostępu do Internetu z LAN;
   - weryfikacja procedur zarządzania siecią LAN.

5) Bezpieczeństwo urządzeń sieciowych

a) badanie odporności urządzeń na ataki z poziomu Internetu;

b) wskazanie potencjalnych skutków ataku dla znalezionych luk i określenie ich krytyczności;

c) wskazanie potencjalnych, dodatkowych metod ochrony sieci;

d) analiza podatności na ataki;

e) skanowanie portów TCP / UDP;

f) skanowanie hostów aktywnych w danej podsieci;

g) określenie ścieżki sieciowej do urządzenia;

h) próba detekcji typu oraz wersji usług sieciowych działających w systemie;

i) próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu;

j) próba komunikacji w obrębie protokołu ICMP;

k) próba generacji pakietów o dużym rozmiarze (np. powiększonych pakietów ICMP echo).

6) Testy bezpieczeństwa VPN (IPsec)

a) badanie poziomu bezpieczeństwa systemów klasy VPN;

b) weryfikacja możliwości użycia systemów klasy VPN jako punkt pośredniego do ataku na infrastrukturę IT;
c) określenie realnego zabezpieczenia komunikacji sieciowej oferowanej przez wdrożoną u Zamawiającego implementację VPN;
d) próba wykrycia aktywności serwera VPN;
e) próba wykrycia rodzaju wykorzystywanego rozwiązania VPN (dostawcy sprzętu);
f) próba inicjowania tunelu z różnymi algorytmami kryptograficznymi (szyfry symetryczne, funkcje skrótu, metoda uwierzytelniania, grupa DH);
g) skanowanie portów oraz podatności na koncentratorze VPN;
h) weryfikacja wykorzystanych trybów połączenia (transport, tunnel, ESP, AH);
i) weryfikacja przyjętych metod uwierzytelniania (np. PKI, hasła jednorazowe);
j) weryfikacja przyjętych polityk bezpieczeństwa dla urządzeń klienckich korzystających z VPN (pod względem możliwości ataku na infrastrukturę VPN - inicjowanych z urządzeń klienckich);
k) podstawowa analiza architektury sieci – pod względem rozmieszczenia komponentów.

7) Audyt procesów zarządczych IT w zakresie serwerów, sieci, infrastruktury, baz danych, aplikacji, obejmujący:
a) podział ról i odpowiedzialności za zarządzanie w badanym obszarze
b) analiza architektury w badanym obszarze
c) procesy zarządzania zmianą
d) procesy obsługi incydentów
e) procesy wdrażania nowych rozwiązań
f) procesy wycofywania
g) procesy utrzymania

8) Audyt na zgodność z krajowymi ramami interoperacyjności, obejmujący:
a) Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną
   - usługi elektroniczne
   - centralne repozytorium wzorów dokumentów elektronicznych
   - model usługowy
   - współpraca systemów teleinformatycznych z innymi systemami
   - obieg dokumentów w urzędzie
   - formaty danych udostępniane przez systemy teleinformatyczne
b) system zarządzania bezpieczeństwem informacji w systemach teleinformatycznych
   - dokumenty z zakresu bezpieczeństwa informacji, zaangażowanie kierownictwa podmiotu
   - analiza zagrożeń związanych z przetwarzaniem informacji
   - inwentaryzacja sprzętu i oprogramowania informatycznego
   - zarządzanie uprawnieniami do pracy w systemach informatycznych
   - szkolenia pracowników zaangażowanych w proces przetwarzania informacji
   - praca na odległość i mobilne przetwarzanie danych
   - serwis sprzętu informatycznego i oprogramowania
   - procedury zgłaszania incydentów naruszenia BI
   - audyt wewnętrzny z zakresu bezpieczeństwa informacji
   - kopie zapasowe

- projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych
- zabezpieczenia techniczno-organizacyjne dostępu do informacji
- zabezpieczenia techniczno-organizacyjne systemów informatycznych
- rozliczalność działań w systemach teleinformatycznych

c) zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych

II. Raporty

1. Wynikiem przeprowadzonych audytów i testów będzie raport poaudytowy zawierający:
   1) przedmiot, cel i zakres audytu;
   2) datę rozpoczęcia audytu;
   3) opis przyjętej metodyki;
   4) raport dla kierownictwa obejmujące syntezę wyników audytu i ocenę poziomu spełnienia wymogów KRI / UoKSC regulacji wewnętrznych dot. bezpieczeństwa informacji Zamawiającego oraz ocenę bezpieczeństwa systemu informatycznego w tym podsumowanie zidentyfikowanych słabości / nieprawidłowości, a także główne rekomendacje dotyczące poprawy bezpieczeństwa informacji, danych i systemu informatycznego;
   5) raport szczegółowy zawierający dokładny opis zidentyfikowanych nieprawidłowości w szczególności:
      a) wskazujący dokładne miejsca, w których występują realne bądź potencjalne problemy z bezpieczeństwem informacji;
      b) zawierający wyniki audytów, w tym testów i ich interpretację - każde ustalenie musi odnosić się do konkretnych przypadków słabości/nieprawidłowości popartych zgromadzonymi dowodami audytowymi, które będą stanowiły załącznik do raportu;
      c) opisy błędów, informacje jakich narzędzi użyto do odnalezienia błędu, opis warunków, które są konieczne aby doszło do błędu;
      d) plik proof of concept, pozwalający na reprodukcję błędu;
      e) zawierający rekomendacje w zakresie eliminacji zidentyfikowanych słabości/nieprawidłowości oraz poprawy poziomu bezpieczeństwa, w tym wskazanie działań korygujących i/lub doskonalących;

      Ocena, ustalenia i rekomendacje muszą być ze sobą jasno powiązane i łatwo identyfikowalne.
   6) propozycje zmian w treści regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI) Zamawiającego wraz z proponowaną treścią nowych (zmienionych lub dodanych) zapisów;
   7) datę sporządzenia raportu;
   8) imiona i nazwiska audytorów realizujących zadanie oraz ich podpisy.
2. Raport musi zawierać podział podatności ze względu na ryzyko, wpływ wykrytej podatności na poufność, integralność i dostępność informacji (poziom krytyczności), prawdopodobieństwo wykorzystania podatności, złożoność (trudność) wprowadzenia naprawy – usunięcia podatności.
3. Raport z audytu musi być podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST.

4. Raport w formie edytowalnej i pdf, przesyłany drogą elektroniczną musi być zaszyfrowany przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 9-znakowym hasłem jednorazowym (zawierającym małe i duże litery, cyfry i znaki specjalne) przesłanym przez Wykonawcę alternatywny kanał komunikacji w terminie do 14 dni od daty zakończenia audytu w siedzibie Zamawiającego.

Załącznik nr 2 do Zapytania Ofertowego

WZÓR UMOWY

Zawarta w dniu ..... r. w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego pn. „**Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych**", realizowanego w ramach projektu "Cyberbezpieczny Urząd Gminy Ślemień" finansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe" Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa", pomiędzy:

Gminą Ślemień z siedzibą ul. ....., ...-..... ....., NIP ....., reprezentowaną przez ..... – Wójta ....., przy kontrasygnacie .....– ....., zwaną dalej **Zamawiającym**

a firmą:

zarejestrowaną w ..... pod numerem:.....
NIP: ....., reprezentowaną przez: ..... zwaną dalej **Wykonawcą**,

zwanych dalej Stronami, została zawarta umowa następującej treści;

Podstawę zawarcia niniejszej umowy, zwanej dalej „**Umową**" stanowi udzielenie zamówienia publicznego w trybie zapytania ofertowego.

§1
Przedmiot Umowy

1. Przedmiotem Umowy jest usługa przeprowadzenia audytu bezpieczeństwa wdrożonego systemu zarządzania bezpieczeństwem informacji wraz z wykonaniem testów penetracyjnych zgodnie z opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do Umowy.

§2
Termin wykonania Umowy

1. Wykonawca zobowiązuje się wykonać przedmiot Umowy w terminie do **60 dni** od daty podpisania Umowy.
2. Za termin wykonania przedmiotu zamówienia uważa się datę podpisania protokołu odbioru.

§3
Nadzór nad realizacją Umowy

1. Nadzór nad realizacją postanowień Umowy ze strony Zamawiającego prowadził będzie:
   ....., tel. ..... email: .....– przedstawiciel Zamawiającego.
2. Przedstawicielem Wykonawcy w zakresie realizacji Umowy będzie:
   ....., tel. ..... email: ..... – przedstawiciel Wykonawcy.
3. Wykonawca może dokonać zmiany swojego przedstawiciela, zawiadamiając o tym Zamawiającego na piśmie. Zmiana jest skuteczna od chwili doręczenia przedstawicielowi Zamawiającemu informacji o zmianie i nie stanowi zmiany Umowy.

§4
Sposób realizacji przedmiotu Umowy

1. Zamawiający przekaże Wykonawcy materiały, stanowiące podstawę do realizacji przedmiotu Umowy.
2. Wszelkie szczegółowe warunki przedmiotu Umowy znajdują się w Zapytaniu Ofertowym.
3. Wykonawca zobowiązuje się wykonać przedmiot Umowy z zachowaniem należytej staranności i rzetelności zawodowej, zgodnie z postanowieniami niniejszej Umowy.
4. Przedmiot Umowy musi być wykonany przez osoby skierowane do realizacji zamówienia wskazane w ofercie.

5. Usługi niepełne lub niezgodne z Zapytaniem Ofertowym traktowane są jako pozostawanie przez Wykonawcę w opóźnieniu.
6. Wykonawca zobowiązuje się wykonać prace będące przedmiotem niniejszej Umowy z zachowaniem należytej staranności i rzetelności zawodowej, zgodnie z postanowieniami niniejszej Umowy oraz specyfikacji istotnych warunków zamówienia.
7. Wykonawca ma prawo do zmiany osób wskazanych w wykazie osób skierowanych przez Wykonawcę do realizacji zamówienia z zastrzeżeniem, iż osoby te muszą posiadać kwalifikacje zawodowe i uprawnienia co najmniej równe określonym przez Wykonawcę w wyżej wymienionym wykazie, po poinformowaniu Zamawiającego o zamiarze zmiany i uzyskaniu jego pisemnej akceptacji. Zmiana osób będzie dokonana w formie aneksu.
8. Wykonawca oświadcza, że w ramach swojego personelu dysponuje osobami posiadającymi niezbędną wiedzę i umiejętności konieczne do właściwego wykonania Umowy, a w szczególności, że dysponuje personelem o wszystkich wymaganych profilach kompetencji zawodowych niezbędnych do realizacji przedmiotu Umowy.
9. Wykonawca ponosi odpowiedzialność za działania i zaniechania podwykonawców, dalszych podwykonawców - jeżeli Wykonawca będzie wykonywał przedmiot Umowy przy pomocy podwykonawców, dalszych podwykonawców – jak za swoje własne.

§5
Zachowanie tajemnicy i poufność informacji

1. Wykonawca zobowiązuje się do:
   a) zachowania w tajemnicy wszelkich informacji o Zamawiającym i przedmiocie niniejszej Umowy, jakie uzyskał w związku z jej realizacją,
   b) przestrzegania wytycznych Zamawiającego o ochronie udostępnionych informacji,
   c) przestrzegania przepisów ustawy o ochronie danych osobowych.
2. Wszelkie materiały przekazane Wykonawcy przez Zamawiającego w związku z wykonaniem przedmiotu Umowy, z wyłączeniem udostępnionych w przetargu, a także powstałe w wyniku jej wykonania (pisemne, graficzne, zapisane w formie elektronicznej i w inny sposób) są poufne i nie mogą być bez uprzedniej pisemnej zgody Zamawiającego udostępniane osobom trzecim ani ujawniane w inny sposób.
3. Wykonawca odpowiada za zachowanie poufności, o której mowa w ust. 1, przez wszystkie osoby, którymi posługuje się przy wykonaniu przedmiotu Umowy.
4. Wykonawca zobowiązuje się zwrócić Zamawiającemu wszelkie materiały otrzymane od Zamawiającego w związku z realizacją przedmiotu Umowy, niezwłocznie po otrzymaniu takiego żądania.
5. Wykonawca zwolniony jest z obowiązku zachowania poufności jeżeli informacje, co do których taki obowiązek istniał muszą być ujawnione zgodnie z przepisami prawa lub postanowieniami sądów lub innych upoważnionych organów państwa lub muszą być ujawnione w celu wykonania przedmiotu Umowy, a Wykonawca uzyskał pisemną zgodę Zamawiającego na ich ujawnienie.
6. Obowiązek zachowania poufności jest nieograniczony w czasie, jego uchylenie może być dokonane wyłącznie przez Zamawiającego w formie pisemnej.

§6
Warunki odbioru

1. Odbiór przedmiotu Umowy następuje na podstawie protokołu odbioru.
2. Po zakończeniu realizacji przedmiotu Umowy Wykonawca zgłasza gotowość do odbioru przedmiotu Umowy.
3. Warunkiem koniecznym do poprawnego zgłoszenia gotowości do odbioru końcowego jest przekazanie Zamawiającemu kompletnego raportu poaudytowego.
4. Zamawiający po otrzymaniu zgłoszenia gotowości odbioru powinien dokonać odbioru w terminie nie przekraczającym 7 dni roboczych.
5. W ramach czynności kontrolnych, Zamawiający sprawdza zgodność przedmiotu Umowy z wymaganiami określonymi w Umowie wraz z załącznikami. Pozytywny wynik kontroli jest podstawą podpisania protokołu odbioru.
6. Data podpisania protokołu odbioru stanowi datę wykonania i odbioru przedmiotu Umowy.

7. Jeżeli w toku czynności kontrolnych stwierdzone zostanie, że przekazany przedmiot Umowy jest niezgodny z zapisami zawartymi w Umowie oraz załącznikach do Umowy, Zamawiający przerywa odbiór. W takim przypadku Wykonawca zobowiązany jest do poprawy przedmiotu Umowy i ponownego oddania go do kontroli w terminie 7 dni. Ust. 2 do 4 mają odpowiednie zastosowanie.
8. Termin kontroli i poprawy przedmiotu Umowy będzie wliczany do terminu faktycznej realizacji przedmiotu Umowy przez Wykonawcę i objęty karami Umownymi określonymi w §8 ust.1.lit. a.

§7
Wynagrodzenie Wykonawcy

1. Za wykonanie przedmiotu Umowy, strony Umowy ustalają wynagrodzenie brutto w kwocie w wys. .....zł w tym podatek VAT według obowiązującej stawki.
2. Oferowana cena obejmuje wszystkie koszty realizacji zamówienia.
3. Cena obejmuje całkowitą należność jaką Zamawiający zobowiązany jest zapłacić za wykonanie przedmiotu Umowy. Cena oferowana zawiera wszystkie elementy wykonania zamówienia.
4. Rozliczenie przedmiotu Umowy nastąpi fakturą końcową. Podstawę wystawienia faktury końcowej stanowi protokół odbioru przedmiotu Umowy podpisany przez obie strony wraz z załącznikami, o których mowa w § 6 ust.3 niniejszej Umowy.
5. Faktura ma zawierać wyszczególnienie przedmiotu Umowy.
6. Faktura płatna będzie przelewem w terminie do 30 dni od daty otrzymania przez Zamawiającego poprawnie wystawionej faktury.
7. Płatności faktur będą dokonywane przez Zamawiającego przelewem z rachunku bankowego na rachunek Wykonawcy w banku: ..... nr rachunku: ..... . Warunkiem zapłaty wynagrodzenia przez Zamawiającego na wskazany przez Wykonawcę rachunek jest figurowanie podanego rachunku w elektronicznym wykazie czynnych podatników VAT, prowadzonym przez Szefa Krajowej Administracji Skarbowej (tzw. biała lista podatników VAT).
8. W przypadku wskazania na fakturze rachunku bankowego nieujawnionego w wykazie podatników VAT, Zamawiający uprawniony będzie do dokonania płatności na inny rachunek bankowy ujawniony w wykazie podatników VAT lub do zapłaty na rachunek bankowy podany na fakturze, z jednoczesnym powiadomieniem właściwego naczelnika urzędu skarbowego.
9. Za dzień zapłaty wynagrodzenia uważa się dzień obciążenia rachunku bankowego Zamawiającego. W przypadku konsorcjum, płatność nastąpi na konto lidera konsorcjum.
10. W razie nieterminowej zapłaty faktury Zamawiający zobowiązuje się do zapłaty ustawowych odsetek.
11. Zamawiający dopuszcza wystawianie faktur w formie elektronicznej i przesyłanie ich Zamawiającemu pocztą elektroniczną na adres: ..... oraz do wiadomości osobie sprawującej ze strony Zamawiającego nadzór nad realizację Umowy (zgodnie z §3 ust.1 Umowy). W przypadku niewysłania faktury na jeden ze wskazanych adresów Zamawiający nie będzie uznawał faktury elektronicznej za prawidłowo doręczonej.

§8
Kary umowne

1. W przypadku niewykonania Umowy lub nienależytego wykonania Umowy, strony ustalają zapłatę kar umownych w wypadkach i wysokości określonych w Umowie.
2. Wykonawca płaci Zamawiającemu kary Umowne:
   a) za nieterminowe wykonanie przedmiotu Umowy w wysokości 0,1% wynagrodzenia umownego brutto określonego §7 ust. 1 za każdy rozpoczęty dzień,
   b) z tytułu odstąpienia od Umowy z przyczyn występujących po stronie Wykonawcy w wysokości 10% wynagrodzenia umownego brutto określonego w §7 ust. 1.
3. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującego mu wynagrodzenia za wykonanie przedmiotu Umowy, a w przypadku braku możliwości potrącenia będą płatne przelewem na konto bankowe Zamawiającego wskazane w wezwaniu do zapłaty, w terminie 7 dni od daty otrzymania przez Wykonawcę wezwania do ich zapłaty.

4. Łączna wysokość kar umownych, o których mowa w ust. 2, nie przekroczy kwoty stanowiącej 20% wartości Umowy brutto określonej w §7 ust.1.
5. Strony zastrzegają sobie prawo dochodzenia odszkodowania uzupełniającego, przewyższającego wysokość zastrzeżonych kar umownych.

§9
Prawa autorskie

1. W ramach wynagrodzenia, o którym mowa w §7 ust. 1, Wykonawca przenosi na Zamawiającego majątkowe prawa autorskie do wszelkich utworów powstałych w wykonaniu lub w związku z wykonaniem Umowy. Wykonawcy nie będzie przysługiwało odrębne wynagrodzenie za korzystanie z utworu na polach eksploatacji określonych w ust.2
2. Przeniesienie majątkowych praw autorskich, o których mowa ust. 1, następuje z chwilą przekazania utworu Zamawiającemu, bez ograniczeń co do terytorium, czasu lub liczby egzemplarzy, na wszelkich znanych polach eksploatacji, w szczególności:
   1) w zakresie utrwalania i zwielokrotniania utworu - wytwarzanie określoną techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
   2) w zakresie obrotu oryginałem albo egzemplarzami, na których utwór utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;
   3) w zakresie rozpowszechniania utworu w sposób inny niż określony w lit. b) - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym;
   4) w zakresie używania;
   5) w zakresie wykorzystywania w całości lub części utworów powstałych w wyniku wykonywania Umowy lub w związku z wykonywaniem Umowy oraz dokonywania w nich zmian;
   6) wprowadzenie do pamięci komputera lub do sieci komputerowej; tłumaczenie na różne języki, zmiany wielkości, układu, treści lub jakichkolwiek innych zmian całości lub części utworów;
   7) w zakresie wykorzystania utworu w procesie realizacji projektu, w postępowaniach o udzielenie zamówień publicznych, w szczególności poprzez włączenie utworu lub jego części do postępowań oraz udostępnianie utworu i jego części wszystkim zainteresowanym tymi postępowaniami.
3. Wykonawca oświadcza i zapewnia, że wykonując przedmiot Umowy nie naruszy praw osób trzecich i przekaże Zamawiającemu utwory powstałe w wyniku wykonywania Umowy lub w związku z jej wykonywaniem w stanie wolnym od obciążeń prawami osób trzecich.
4. Wykonawca jest odpowiedzialny za wszelkie wady fizyczne i prawne utworów dostarczonych w wykonaniu Umowy, a w szczególności za ewentualne roszczenia osób trzecich wynikające z naruszenia praw autorskich.
5. W przypadku wystąpienia przez osobę trzecią przeciwko Wykonawcy z tytułu naruszenia jej praw autorskich, Wykonawca, niezależnie od odpowiedzialności odszkodowawczej wobec Zamawiającego, zobowiązuje się do całkowitego zaspokojenia słusznych roszczeń osób trzecich oraz do zwolnienia Wykonawcy od obowiązku świadczenia z tego tytułu.
6. Z chwilą przekazania utworu Zamawiającemu, Zamawiający nabywa własność wszystkich egzemplarzy nośników, na których utwór został utrwalony.

§10
Odstąpienie i rozwiązanie Umowy

1. Zamawiający może odstąpić od Umowy:
   a) w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie Umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający

może odstąpić od Umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach. W takim przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy;

b) w przypadku powtarzającego się naruszenia postanowień niniejszej Umowy, z zastrzeżeniem, że odstąpienie od Umowy przez Zamawiającego będzie poprzedzone wezwaniem Wykonawcy do realizowania Umowy zgodnie z zawartymi w Umowie postanowieniami.

2. Umowa lub jej część ulega rozwiązaniu w dniu doręczenia drugiej Stronie pisma informującego o odstąpieniu wraz z uzasadnieniem.
3. Postanowienia niniejszego paragrafu nie ograniczają praw Stron do odstąpienia od Umowy z przyczyn określonych w przepisach powszechnie obowiązujących, w tym w szczególności uprawnień Zamawiającego wynikających z art. 456 ustawy Pzp.

§11
Zmiany w Umowie

1. Strony dopuszczają możliwość zmiany postanowień Umowy w stosunku do treści oferty, na podstawie, której dokonano wyboru wykonawcy w następujących przypadkach:
   1) zmiany terminu realizacji przedmiotu Umowy, w następstwie:
      a) siły wyższej - rozumianej jako wystąpienie zdarzenia nadzwyczajnego, zewnętrznego, niemożliwego do przewidzenia i zapobieżenia, którego nie dało się uniknąć nawet przy zachowaniu najwyższej staranności, a które uniemożliwia Wykonawcy wykonanie przedmiotu Umowy. W razie wystąpienia siły wyższej Strony Umowy zobowiązane są dołożyć wszelkich starań w celu ograniczenia do minimum opóźnienia w wykonywaniu swoich zobowiązań Umownych, powstałego na skutek działania siły wyższej. (Pod pojęciem siły wyższej rozumie się w szczególności zdarzenia i okoliczności takie jak: klęska żywiołowa, działania wojenne, rebelie, terroryzm, rewolucja, powstanie, inwazja, bunt, zamieszki, strajk spowodowany przez inne osoby, niezwiązane z realizacją przedmiotu Umowy, COVID, itp.),
      b) okoliczności leżących po stronie Zamawiającego i nie wynikających z przyczyn leżących po stronie Wykonawcy (np. wstrzymanie, zawieszenie, przerwa w realizacji),
      c) przestojów i opóźnień zawinionych przez Zamawiającego,
      d) wystąpienia okoliczności, których strony Umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności,
      e) przyczyn niezależnych od którejkolwiek ze stron, które w szczególności dotyczyć będą: uwarunkowań formalno-prawnych;
   2) zmiana danych związana z obsługą administracyjno-organizacyjną Umowy (danych teleadresowych Wykonawcy; Zamawiającego, zmiana rachunku bankowego) - zmiana ta następuje poprzez pisemne zgłoszenie tego faktu drugiej stronie i nie wymaga zawarcia aneksu do Umowy,
   3) przekształcenie Wykonawcy w związku z sukcesją generalną, przekształceniami, dziedziczeniem spółek handlowych zgodnie z KSH, a także sukcesją z mocy prawa, zgodnie z obowiązującymi przepisami (następstwa prawne) winno nastąpić w formie aneksu do Umowy.
2. Wszystkie powyższe postanowienia stanowią katalog zmian, na które Zamawiający może wyrazić zgodę. Nie stanowią jednocześnie zobowiązania do wyrażenia takiej zgody.
3. W sytuacji wystąpienia okoliczności, o których wyżej mowa, każda ze stron może wystąpić z wnioskiem zawierającym:
   1) opis propozycji zmiany, w tym wpływ na terminy wykonania,
   2) uzasadnienie zmiany.
4. Wszelkie zmiany i uzupełnienia niniejszej wymagają formy pisemnej pod rygorem nieważności - aneks do Umowy, z zastrzeżeniem przypadków określonych w niniejszym paragrafie, w których wskazano, że nie jest wymagane zawarcie aneksu do Umowy.
5. Jeżeli postanowienia niniejszej Umowy są albo staną się nieważne albo nieskuteczne, lub Umowa zawierać będzie lukę, nie narusza to ważności i skuteczności pozostałych postanowień Umowy. Zamiast nieważnych albo nieskutecznych postanowień lub jako wypełnienie luki obowiązywać będzie odpowiednia regulacja, która – jeżeli

tylko będzie to prawnie dopuszczalne – w sposób możliwie bliski odpowiadać będzie temu, co Strony ustaliły albo temu, co by ustaliły, gdyby zawarły takie postanowienie, pod warunkiem, że jeżeli całość Umowy bez nieważnych albo nieskutecznych postanowień zachowuje rozsądną treść.

§12

Postanowienia końcowe

1. Strony ustalają, że w sprawach nieuregulowanych postanowieniami niniejszej Umowy będą miały zastosowanie przepisy prawa polskiego, w szczególności Kodeksu cywilnego.
2. Strony zgodnie ustalają, że Wykonawca nie może dokonać cesji jakichkolwiek praw lub obowiązków wynikających z tej Umowy, bez pisemnej zgody Zamawiającego.
3. Zamawiający oraz Wykonawca zarówno w trakcie obowiązywania niniejszej Umowy, jak również po jej zakończeniu, są zobowiązani do zachowania w tajemnicy wszelkich informacji dotyczących warunków i realizacji niniejszej Umowy, z wyłączeniem informacji podlegających obowiązkowi podania ich do wiadomości publicznej.
4. Strona Umowy, która naruszyła postanowienia ust. 3 odpowiada za wyrządzenie szkody na zasadach ogólnych.
5. Spory wynikłe na tle realizacji niniejszej Umowy rozstrzygane będą przez sąd miejscowo właściwy dla siedziby Zamawiającego.

§13

Załączniki

Integralną część Umowy stanowią Załączniki:

1) Załącznik nr 1 – Opis Przedmiotu Zamówienia
2) Załącznik nr 2 – Oferta Wykonawcy
3) Załącznik nr 3 – Umowa powierzenia przetwarzania danych osobowych

Zamawiający	Wykonawca
.....	.....

Załącznik nr 3 do Zapytania Ofertowego

Wykonawca:

.....

.....
(pełna nazwa/firma, adres, w zależności od podmiotu NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

.....
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Gmina Ślemień
ul. Krakowska 148, 34–323 Ślemień

FORMULARZ OFERTOWY

Nawiązując do postępowania o udzielenie zamówienia publicznego w trybie zapytania ofertowego pn. **„Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych"** - nr referencyjny ZP.271.1.2.2026, realizowanego w ramach projektu " Cyberbezpieczny Urząd Gminy Ślemień" finansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe" Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa", oferujemy wykonanie zamówienia na następujących warunkach.

1. Cena oferty z złotych polskich

   Oferujemy wykonanie przedmiotu zamówienia zgodnie z Opisem Przedmiotu Zamówienia stanowiącym integralną część oferty za:

   cena netto oferty: ..... zł

   podatek VAT: ..... zł

   cena brutto oferty: ..... zł

   słownie: .....

2. Formularz cenowy

NAZWA	CENA NETTO [ZŁ]	ILOŚĆ [SZT.]	WARTOŚĆ NETTO [ZŁ]	PODATEK VAT [ZŁ]	WARTOŚĆ BRUTTO [ZŁ]
Audyt bezpieczeństwa		1			
Testy penetracyjne		1			
SUMA					

3. Termin wykonania zamówienia: – **do 60 dni** od daty zawarcia umowy.

4. Warunki płatności

   4.1. Zapłata należności nastąpi przelewem w terminie 30 dni licząc od daty doręczenia Zamawiającemu prawidłowo wystawionej przez Wykonawcę faktury, na rachunek bankowy Wykonawcy znajdujący się na „białej liście"

   Nazwa Banku: ....., Numer rachunku: .....

   4.2. Za dzień spełnienia świadczenia pieniężnego uważać się będzie dzień obciążenia rachunku w banku Zamawiającego. Wykonawca zamieści na fakturze numer niniejszej Umowy.

5. Niniejszym oświadczam, że:

5.1. firma, którą reprezentuję jest mikroprzedsiębiorstwem /małym przedsiębiorstwem / średnim przedsiębiorstwem[1];

5.2. zapoznałem się ze Specyfikacją Warunków Zamówienia (Zapytanie Ofertowe) i przyjmuję je bez zastrzeżeń;

5.3. przedmiot oferty jest zgodny z przedmiotem zamówienia;

5.4. zawarty w Zapytaniu ofertowym wzór umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku wybrania naszej oferty do zawarcia umowy na warunkach w niej określonych w miejscu i terminie wyznaczonym przez Zamawiającego;

5.5. wybór oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług / wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług i wskazuję: nazwę (rodzaj) towaru, których dostawa będzie prowadziła do powstania obowiązku podatkowego, wartość towaru objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku oraz stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie*

..... ;

** niepotrzebne skreślić*

5.6. przedmiot zamówienia wykonamy siłami własnymi / przy udziale podwykonawców*, którym zamierzamy powierzyć wykonanie następujących części zamówienia i podajemy firmy/nazwy podwykonawców:

L.P.	CZĘŚĆ/ZAKRES ZAMÓWIENIA	NAZWA (FIRMA) PODWYKONAWCY
1		
2		

(*) niepotrzebne skreślić

5.7. wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu*;

(*) W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia z punktu 9 wykonawca nie składa i go wykreśla.

5.8. zapoznałem się z dokumentami zamówienia, w tym dołączoną klauzulą informacyjną FERC i akceptuję ich treść.

....., *dnia* .....

.....

Podpis osoby uprawnionej
do reprezentowania Wykonawcy

[1] *niepotrzebne skreślić*

Zgodnie z zaleceniem Komisji (UE) z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw:

Mikroprzedsiębiorstwo: *przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.*

Małe przedsiębiorstwo: *przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.*

Średnie przedsiębiorstwa: *przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR.*

Załącznik nr 4 do Zapytania Ofertowego

Wykonawca:

.....

.....

(pełna nazwa/firma, adres, w zależności od podmiotu NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

OŚWIADCZENIE

składane w postępowaniu o udzielenie zamówienia publicznego w trybie zapytania ofertowego pn.: **„Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych"** - nr referencyjny ZP.271.1.2.2026, realizowanego w ramach projektu "Cyberbezpieczny Urząd Gminy Ślemień" finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe" Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa".

1. WARUNKI UDZIAŁU W POSTĘPOWANIU

1) Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Specyfikacji warunków zamówienia w Rozdziale V dotyczące zdolności technicznej i zawodowej w zakresie osób skierowanych przez Wykonawcę do realizacji zamówienia publicznego.

2) W celu realizacji zamówienia będę polegał / nie będę polegał * na zdolności innych podmiotów w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w Specyfikacji Warunków Zamówienia w Rozdziale V.

Jeżeli Wykonawca będzie polegał na zdolności innych podmiotów, należy przedstawić – oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby – oświadczenie musi zawierać wszystkie wymagane informacje, należycie wypełnione i podpisane przez dane podmioty.

** niepotrzebne skreślić*

2. PODSTAWY WYKLUCZENIA

1) Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie przesłanek określonych w rozdział V ust.1 Zapytania Ofertowego.

2) Oświadczam, że nie zachodzą wobec mnie przesłanki wykluczenia z postępowania o których mowa wart. 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.

3. OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

Prawdziwość powyższych danych potwierdzam świadomy odpowiedzialności karnej z art. 297 §1 KK.

..... *(miejscowość),* dnia ..... r.

.....

Podpis osoby uprawnionej do reprezentowania Wykonawcy

Załącznik Nr 5 do Zapytania Ofertowego

Wykonawca:

.....

.....
(pełna nazwa/firma, adres, w zależności od podmiotu NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

.....
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

WYKAZ USŁUG

składany w postępowaniu o udzielenie zamówienia publicznego w trybie zapytania ofertowego pod nazwą: **„Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych"** - nr referencyjny ZP.271.1.2.2026, realizowanego w ramach projektu "Cyberbezpieczny Urząd Gminy Ślemień" finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe" Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa".

L.p.	Przedmiot dostawy	Wartość w PLN	Data/daty wykonania	Podmiot, na rzecz którego dostawa została wykonana
1				
2				
(...)				

W załączeniu:

dowody określające, czy te dostawy zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie Wykonawcy.

..... *(miejscowość),* dnia ..... r.

.....
Podpis osoby uprawnionej
do reprezentowania Wykonawcy

Załącznik nr 6 do Zapytania Ofertowego

Wykonawca:

.....

.....
(pełna nazwa/firma, adres, w zależności od podmiotu NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

.....
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

WYKAZ OSÓB

składany w postępowaniu o udzielenie zamówienia publicznego w trybie zapytania ofertowego pod nazwą: **„Przeprowadzenie audytu bezpieczeństwa i testów penetracyjnych"** - nr referencyjny ZP.271.1.2.2026, realizowanego w ramach projektu "Cyberbezpieczny Urząd Gminy Ślemień" finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe" Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa"

L.p.	Imię i nazwisko	Kwalifikacje*	Doświadczenie**	Zakres wykonywanych czynności	Podstawa do dysponowania przez Wykonawcę
1					
2					
3					
(...)					

** Informacje na temat kwalifikacji zawodowych, uprawnień i wykształcenia niezbędnych do wykonania zamówienia publicznego Wykonawca określi rodzaj posiadanych uprawnień. Zamawiający wymaga złożenia kserokopii uprawnień wraz z ofertą.*

*** Wykonawca określi staż pracy określony w latach. Jako staż pracy przyjmuje się okres czasu od momentu uzyskania uprawnień.*

..... *(miejscowość),* dnia ..... r.

.....
Podpis osoby uprawnionej do reprezentowania Wykonawcy

Załącznik nr 8 - Klauzula informacyjna FERC

Klauzula informacyjna FERC

W celu wykonania obowiązku nałożonego w drodze art. 13 i 14 RODO, w związku z art. 88 ustawy wdrożeniowej, informujemy o zasadach przetwarzania Państwa danych osobowych:

Administrator danych

Odrębnymi administratorami Państwa danych są:

1. Minister Funduszy i Polityki Regionalnej (dalej jako MFiPR), w zakresie w jakim pełni funkcję Instytucji Zarządzającej (IZ) Funduszami Europejskimi na Rozwój Cyfrowy 2021-2027 (dalej jako FERC) z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa,
2. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Instytucji Pośredniczącej (IP) FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa,
3. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Beneficjenta FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.

Cel przetwarzania danych

Państwa dane osobowe będziemy przetwarzać w związku z realizacją FERC, w szczególności w związku z naborem 2.2 FERC. Podanie danych jest dobrowolne, ale konieczne do realizacji ww. celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

Podstawa przetwarzania

Będziemy przetwarzać Państwa dane osobowe w związku z tym, że:

1. Zobowiązuje nas do tego **prawo** (art. 6 ust. 1 lit. c RODO):
   1) art. 87 ustawy wdrożeniowej,
   2) art. 61 ustawy z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079),
   3) ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (tekst jednolity Dz.U. z 2023 r. poz. 775 z późn. zm.),

4) art. 206 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity Dz. U. z 2022 r. poz. 1634, z późn. zm.),
5) Porozumienie trójstronne w sprawie systemu realizacji programu „Fundusze Europejskie na Rozwój Cyfrowy 2021-2027" z 2.02.2023 r.,
6) rozporządzenia Ministra Cyfryzacji z dnia 16 lutego 2023 r. w sprawie udzielania pomocy na rozwój infrastruktury szerokopasmowej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (Dz. U. z 2023 r. poz. 405),

2. Wykonujemy zadania w interesie publicznym lub sprawujemy powierzoną nam władzę publiczną (art. 6 ust. 1 lit. e RODO),
3. Przygotowujemy i realizujemy **umowy**, których są Państwo stroną, a przetwarzanie danych osobowych jest niezbędne do ich zawarcia i wykonania (art. 6 ust. 1 lit. b RODO).

Rodzaje przetwarzanych danych

Możemy przetwarzać następujące rodzaje Państwa danych:

1. dane identyfikacyjne, wskazane w art. 87 ust. 2 pkt 1 ustawy wdrożeniowej, w tym: imię, nazwisko, adres, adres poczty elektronicznej, numer telefonu, numer faksu, PESEL, REGON, wykształcenie, identyfikatory internetowe,
2. dane związane z zakresem uczestnictwa osób fizycznych w projekcie, wskazane w art. 87 ust. 2 pkt 2 ustawy wdrożeniowej, w tym w szczególności: wynagrodzenie, formę i okres zaangażowania w projekcie,
3. dane osób fizycznych widniejące na dokumentach potwierdzających kwalifikowalność wydatków, wskazane w art. 87 ust. 2 pkt. 3 ustawy wdrożeniowej, m.in. numer rachunku bankowego, doświadczenie zawodowe, numer uprawnień budowlanych, numer księgi wieczystej,
4. dane dotyczące wizerunku i głosu osób uczestniczących w realizacji Programu lub biorących udział w wydarzeniach z nim związanych.

Dane pozyskujemy bezpośrednio od osób, których one dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację FERC w tym w szczególności od wnioskodawców, beneficjentów, partnerów.

Dostęp do danych osobowych

Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy MFiPR oraz CPPC. Ponadto Państwa dane osobowe mogą być powierzane lub udostępniane:

1. podmiotom, w tym ekspertom, o których mowa w art. 80 ustawy wdrożeniowej, którym zleciliśmy wykonywanie zadań w ramach realizacji FERC,
2. instytucji audytowej, o której mowa w art. 71 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,
3. instytucjom Unii Europejskiej (UE) lub podmiotom, którym UE powierzyła zadania dotyczące wdrażania FERC;
4. podmiotom, które wykonują dla nas usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym.

Okres przechowywania danych

Będziemy przechowywać Państwa dane osobowe zgodnie z przepisami o narodowym zasobie archiwalnym i archiwach, do momentu zakończenia realizacji przez IZ/IP/Beneficjenta wszelkich zadań związanych z realizacją i rozliczeniem FERC, z zastrzeżeniem przepisów, które mogą przewidywać dłuższy termin przeprowadzania kontroli, a ponadto przepisów dotyczących pomocy publicznej i pomocy *de minimis* oraz przepisów dotyczących podatku od towarów i usług.

Prawa osób, których dane dotyczą

Przysługują Państwu następujące prawa:

1. dostępu do swoich danych osobowych oraz otrzymania ich kopii (art. 15 RODO),
2. do sprostowania swoich danych (art. 16 RODO),

3. do usunięcia swoich danych (art. 17 RODO) - jeśli dotyczy,
4. do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
5. wniesienia sprzeciwu – wobec przetwarzania swoich danych (art. 21 RODO) - jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO,
6. wniesienia skargi do organu nadzorczego (art. 77 RODO), tj. Prezesa Urzędu Ochrony Danych Osobowych, w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO lub inne przepisy prawa regulujące kwestię ochrony danych osobowych.

Zautomatyzowane podejmowanie decyzji

Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Przekazywanie danych do państwa trzeciego

Nie zamierzamy przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej innej niż Unia Europejska. W przypadku konieczności przekazania Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej zapewniamy, że odbędzie się to z zachowaniem warunków określonych w art. 45 lub 46 RODO.

Kontakt z administratorem danych i Inspektorem Ochrony Danych

Jeśli mają Państwo pytania dotyczące przetwarzania przez CPPC danych osobowych, prosimy kontaktować z Inspektorami Ochrony Danych Osobowych (dalej jako IOD) w następujący sposób:

1. IOD MFiPR:
   1) pocztą tradycyjną kierując korespondencję na adres: ul. Wspólna 2/4, 00-926 Warszawa,
   2) elektronicznie na adres e-mail: **IOD@mfipr.gov.pl**,
2. IOD CPPC:
   1) pocztą tradycyjną kierując korespondencję na adres: ul. Spokojna 13A, 01-044 Warszawa,
   2) elektronicznie na adres e-mail: **bezpieczenstwo@cppc.gov.pl**.

Podstawa prawna:

1. ustawa wdrożeniowa - ustawa z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r., poz. 1079),
2. RODO - 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 (Dz. Urz. UE. L 119 z 4 maja 2016 r., s.1-88; Dz. Urz. UE L 127 z 23 maja 2018, str. 2 oraz Dz. Urz. UE L 74 z 4 marca 2021, str. 35).