



ZAPYTANIE OFERTOWE

Opracowanie strategicznych i szczegółowych uregulowań w zakresie bezpieczeństwa informacji przez zaprojektowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, w tym Polityki Bezpieczeństwa Informacji.

dla postępowania prowadzonego z wyłączeniem przepisów ustawy – Prawo zamówień publicznych o wartości poniżej 130 000 zł netto

1. Dane Zamawiającego:

Narodowy Instytut Wolności
- Centrum Rozwoju Społeczeństwa Obywatelskiego
00-124 Warszawa
al. Jana Pawła II 12
NIP: 7010780575
strona internetowa: www.niw.gov.pl

Osoba do kontaktu: Ewelina Jadachowska e-mail ejadachowska@niw.gov.pl tel. 22 468 44 07

2. Opis przedmiotu zamówienia:

Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Urzędu poprzez opracowanie strategicznych i szczegółowych uregulowań w zakresie bezpieczeństwa informacji przez zaprojektowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, w tym Polityki Bezpieczeństwa Informacji.

Informacje ogólne o środowisku Zamawiającego:

- 1) Przetwarzanie informacji odbywa się w Warszawie, w 1 budynku;
- 2) Informacje przetwarzane są w formie papierowej oraz systemach informatycznych. Zamawiający zatrudnia 60 osób (12 komórek organizacyjnych);
- 3) Środowisko teleinformatyczne zawiera obecnie:
 - a) serwery zewnętrzne (kolokacja);
 - b) serwery wewnętrzne;
 - c) systemy/aplikacje internetowe (zasoby wykonawców zewnętrznych):
 - Baza sprawozdań organizacji pożytku publicznego
 - System Obsługi Dotacji
 - System Obsługi Wolontariatu.

ZAKRES ZAMÓWIENIA

1. Zaprojektowanie dokumentów, procedur i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym Polityki Bezpieczeństwa Informacji (PBI).

Usługa powinna obejmować swoim zakresem:

- etap I – audyt przedwdrożeniowy w Instytucie;
- etap II – klasyfikacja informacji przetwarzanych w Instytucie;
- etap III – szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Instytucie;



- etap IV – opracowanie dokumentacji SZBI i PBI;
- etap V – szkolenia z zakresu SZBI i PBI dla pracowników i kierownictwa Instytutu;
- etap VI – audyt powdrożeniowy.

Etap I - Audyt przedwdrożeniowy

- Weryfikacja poziomu spełnienia wymagań określonych w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Krajowych Ram Interoperacyjności, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych w Instytucie.
- Wykonawca zbada zgodność działań Zamawiającego z uregulowaniami prawnymi.
- Audyt podlega przeprowadzeniu we wszystkich komórkach organizacyjnych Instytutu.
- Przed rozpoczęciem prac Wykonawca przedstawi Zamawiającemu do akceptacji plan audytu.
- Zakres prac audytu przedwdrożeniowego będzie obejmował co najmniej:
 - zapoznanie się ze strukturą organizacyjną Instytutu;
 - analizę i ocenę dokumentacji wewnętrznej, które Zamawiający udostępni Wykonawcy do analizy;
 - wywiady analityczne z wyznaczonymi przez Zamawiającego pracownikami komórek organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa określonych w Krajowych Ramach Interoperacyjności i wewnętrznych uregulowaniach Instytutu;
 - analizę bezpieczeństwa **zasobów teleinformatycznych Instytutu**
- Wykonawca opracuje i sporządzi raport z przeprowadzonego audytu przedwdrożeniowego, zawierający w szczególności:
 - cel i zakres audytu;
 - szczegółowy opis przeprowadzonych prac;
 - opis poziomu spełnienia każdego z wymagań bezpieczeństwa określonych w Krajowych Ramach Interoperacyjności oraz wewnętrznych uregulowaniach Instytutu;
 - wykaz stwierdzonych niezgodności i rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do każdego z wymagań określonych w Krajowych Ramach Interoperacyjności oraz wewnętrznych uregulowaniach Instytutu;
 - podsumowanie i wnioski.
- Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu. Wykonawca zobowiązany jest do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego.

Etap II - Klasyfikacja informacji

- W ramach procesu klasyfikacji informacji Wykonawca jest zobowiązany do zrealizowania następujących prac:
 - opracowanie modelu podziału informacji przetwarzanych w Instytucie w zależności od poziomu ich wrażliwości i przeznaczenia z uwzględnieniem informacji niejawnych;
 - przeszkolenie pracowników Instytutu w zakresie sposobu klasyfikowania informacji;
 - sklasyfikowanie wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych w Instytucie;
 - opracowanie raportu z procesu klasyfikacji informacji.



- b) Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej przez Wykonawcę metodyki klasyfikowania informacji. Uwagi muszą zostać uwzględnione przez Wykonawcę.
- c) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę dokumentacji. Wykonawca zobowiązany jest do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.

Etap III - Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Instytucie

- a) W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Instytucie, a w szczególności:
 - opracować metodykę szacowania ryzyka spełniającą wymagania Krajowych Ramach Interoperacyjności, optymalną ze względu na charakter działalności Instytutu; Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej metodyki analizy ryzyka, a Wykonawca zobowiązany jest je uwzględnić; ponadto Wykonawca zobowiązany jest do przeprowadzenia procesu szacowania ryzyka zgodnie z wybraną i zatwierdzoną przez Zamawiającego metodyką szacowania ryzyka;
 - opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;
 - przeprowadzić wspólnie z wyznaczonymi pracownikami Instytutu proces szacowania ryzyka, w tym: zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;
 - opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Instytutu;
 - opracować przy współudziale wyznaczonych pracowników Instytutu plan postępowania z ryzykiem.
- b) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę dokumentacji. Wykonawca jest zobowiązany do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.

Etap IV - Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji

- a) Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest zaproponować organizację Systemu Zarządzania Bezpieczeństwem Informacji oraz opracować i przedstawić koncepcję wdrożenia Polityki Bezpieczeństwa Informacji w Instytucie.
- b) Koncepcja będzie w szczególności zawierać mapę dokumentów, stanowiącą szczegółowy wykaz dokumentów z zaznaczeniem ich wzajemnych powiązań, w tym:
 - Dokument Główny Polityki Bezpieczeństwa Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji;
 - Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w Instytucie w tym dla obszaru: teleinformatycznego, spraw osobowych, zabezpieczeń fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw



szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;

- Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.
- c) Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uwagi wniesione przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia SZBI i PBI.
- d) Na podstawie zatwierdzonej przez Zamawiającego koncepcji Wykonawca opracuje wszystkie opisane w koncepcji dokumenty. Dokumenty muszą być zgodne ze wszystkimi wymaganiami prawnymi, którymi podlega Instytut. Jeżeli w czasie realizacji umowy wymagania prawne w zakresie bezpieczeństwa informacji ulegną zmianie, Wykonawca zobowiązany jest dostosować dokumentację PBI do zaistniałych zmian.
- e) Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.

Etap V - Szkolenia z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji

Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji dla wszystkich pracowników Instytutu, obejmujących co najmniej:

- omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z SZBI i PBI;
 - odpowiedzialność za naruszenie zasad SZBI i PBI;
 - zasady zgłaszania i reagowania na incydenty.
- a) Szkolenia dla pracowników zostaną przeprowadzone w formie stacjonarnej lub on-line dla trzech 20-osobowych grup; szkolenie każdej grupy będzie obejmować 6 godzin lekcyjnych w czasie jednego dnia szkolenia.
 - b) Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń.

2. Analiza bezpieczeństwa systemów/aplikacji internetowych funkcjonujących w oparciu o zasoby wykonawców zewnętrznych (zasoby zewnętrzne):

- a) Sprawdzenie architektury sieciowej i serwerowej pod kątem bezpieczeństwa.
- b) Weryfikacja mechanizmów uwierzytelniania / autoryzacji.
- c) W ramach wykonywania testów penetracyjnych aplikacji wymagane jest wykorzystanie obowiązujących standardów bezpieczeństwa. Preferowane są standardy udostępniane przez organizację OWASP (Open Web Application Security Project). Zamawiający dopuszcza możliwość wykorzystania przez Wykonawcę także innych standardów. W takim jednak przypadku Wykonawca jest zobowiązany do uzasadnienia swojego podejścia. Decyzja odnośnie zmian w metodyce jest po stronie Zamawiającego;
- d) Opis rekomendowanych działań zapobiegawczych zmierzających do wyeliminowania podatności lub ograniczenia możliwości ich wykorzystania wraz z określeniem sposobu ich wdrożenia.
- e) W wyniku przeprowadzonej analizy wymagane jest przygotowanie raportu obejmującego streszczenie dokumentu w postaci raportu dla kadry zarządzającej. **Raport powinien obejmować w szczególności:**
 - cel i zakres audytu;



- szczegółowy opis przeprowadzonych prac;
- opis czynności wykonanych podczas testu, w tym odniesienie do zastosowanych standardów,
- opis podejścia do realizacji testów, w szczególności zastosowane do weryfikacji standardy i narzędzia,
- streszczenie dokumentu w postaci raportu dla kadry zarządzającej,
- przyjęty model klasyfikacji ryzyka,
- szczegółowy wykaz wykrytych podatności z opisem metody wykrycia i możliwości wykorzystania podatności,
- kategorię podatności, np.: błędy w kontroli dostępu, ujawnianie, błędy w walidacji wprowadzanych danych,
- klasyfikację ryzyka dla wykrytych podatności,
- opis rekomendowanych działań zapobiegawczych zmierzających do wyeliminowania podatności lub ograniczenia możliwości ich wykorzystania, wraz z określeniem sposobu ich wdrożenia.

Zamawiający zastrzega sobie prawo do wnoszenia uwag do raportu przekazanego przez Wykonawcę. Wykonawca jest zobowiązany do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego.

Zamawiający zastrzega sobie możliwość zmiany treści zapytania ofertowego lub stosownych załączników do zapytania (w tym opisu przedmiotu zamówienia) przed upływem terminu składania ofert, o czym poinformuje wykonawców ubiegających się o zamówienie zamieszczając stosowną informację na stronie internetowej, na której zostało zamieszczone ogłoszenie.

3. Warunki realizacji zamówienia:

1. Wymagany termin realizacji zamówienia: do 20 grudnia 2021 r.
2. Miejsce realizacji zamówienia: siedziba NIW-CRSO
3. Warunki płatności: Płatność nastąpi przelewem na rachunek bankowy wskazany przez Wykonawcę w fakturze, w terminie 21 dni od dnia otrzymania przez Zamawiającego od Wykonawcy prawidłowo wystawionej faktury, wystawionej po uprzednim podpisaniu przez obie strony protokołu odbioru bez zastrzeżeń.

Szczegółowe warunki zamówienia zostały określone w załączniku nr 2 do Zapytania ofertowego – Istotne dla Stron postanowienia, które zostaną wprowadzone do treści umowy

4. Warunki udziału w postępowaniu:

1. **Wykonawca musi spełniać łącznie następujące warunki:**
 - 1) Zaakceptować bez zastrzeżeń wszystkie warunki niniejszego Zapytania ofertowego.
 - 2) Posiadać uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania.
 - 3) Posiadać niezbędną wiedzę i doświadczenie oraz dysponować potencjałem technicznym i osobami zdolnymi do należytego i terminowego wykonania zamówienia. Zamawiający uzna warunek za spełniony, jeżeli
 - a) Wykonawca wykaże, że w okresie ostatnich czterech lat, przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał dla co najmniej:



- **2 usługi polegające na opracowaniu i wdrożeniu Polityki Bezpieczeństwa Informacji lub przygotowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji**, w skład którego wchodzi kompletna dokumentacja Polityki Bezpieczeństwa Informacji; każda ww. usługa o wartości nie mniejszej niż 80 000 PLN brutto, w tym jedna usługa zrealizowana na rzecz podmiotu administracji publicznej;
 - **2 usługi polegające na przeprowadzeniu szacowania ryzyka w obszarze bezpieczeństwa informacji** zgodnie z wymaganiami ISO/IEC 27005 lub PN-ISO/IEC 27005 w organizacji zatrudniającej nie mniej niż 100 osób,
- b) Wykonawca wykaże, że dysponuje lub będzie dysponował osobami zdolnymi do realizacji zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, przy czym co najmniej:
- Jedną osobą skierowaną do realizacji zamówienia, pełniącą rolę kierownika zespołu, posiadającego: wykształcenie wyższe, ważny certyfikat wystawiony przez akredytowaną jednostkę certyfikacyjną, potwierdzający znajomość metodyki PRINCE2 na poziomie Practitioner lub równoważnym oraz posiadający co najmniej 3-letnie doświadczenie w zakresie opracowywania i wdrażania Polityki Bezpieczeństwa Informacji lub Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001;
- 4) Wykonawca niespełniający warunków zostanie z postępowania wykluczony. Spełnianie warunków udziału w postępowaniu będzie oceniane na zasadzie spełnia/nie spełnia.
- 5) Ocena spełnienia ww. warunków zostanie dokonana na podstawie informacji zawartych w Formularzu oferty (załącznik nr 1 do Zapytania ofertowego) oraz załączonych do oferty dokumentów (zgodnie z wykazem w pkt 9 Zapytania ofertowego)

5. Opis kryteriów oceny ofert:

Kryterium – cena. Waga kryterium – 100 %

Zamawiający wybierze ofertę Wykonawcy, który przedstawi najniższą cenę oraz spełni warunki udziału określone w Zapytaniu ofertowym.

UWAGA: Zamawiający informuje, że po dokonaniu czynności badania ofert zastrzega możliwość przeprowadzenia negocjacji dotyczących uzupełnienia i doprecyzowania przedmiotu zamówienia pod względem jakościowym lub zmierzającym do obniżenia cen ofertowych.

Do negocjacji Zamawiający zaprosi wszystkich Wykonawców, którzy złożyli oferty spełniające wymagane w zapytaniu ofertowym warunki.

Po przeprowadzeniu negocjacji Zamawiający może dokonać zmian w opisie przedmiotu zamówienia.

Z przeprowadzonych negocjacji Zamawiający sporządza protokół będący podstawą wyboru oferty i ustalenia warunków realizacji przedmiotu zamówienia.

6. Opis sposobu przygotowania ofert:

1. Każdy Wykonawca może złożyć tylko jedną ofertę w niniejszym postępowaniu.
2. Ofertę stanowi:
 - 1) wypełniony formularz oferty sporządzony zgodnie ze wzorem stanowiącym załącznik nr 1 do Zapytania ofertowego;
 - 2) pełnomocnictwo dla osoby/osób podpisującej ofertę i oświadczenia (jeśli uprawnienie tych osób nie wynika z innych dokumentów dołączonych do oferty);
3. Ofertę należy złożyć w języku polskim, w formie elektronicznej, zapewniającej pełną czytelność jej treści. Oferty nieczytelne zostaną odrzucone.



4. Oferta oraz wszystkie oświadczenia składane przez Wykonawcę w toku postępowania winny być podpisane przez osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy, zgodnie z zasadą reprezentacji wynikającą z postanowień odpowiednich przepisów prawnych bądź umowy, uchwały lub pełnomocnictwa.
5. W przypadku Wykonawców wspólnie ubiegających się o zamówienie (np. konsorcja, spółki cywilne) należy ustanowić pełnomocnika do reprezentowania ich w postępowaniu (do oferty należy dołączyć dokument potwierdzający ustanowienie pełnomocnika).
6. Oferta Wykonawcy winna być podpisana w sposób umożliwiający identyfikację osoby składającej podpis.
7. Wszelkie skreślenia, poprawki, których dokonał Wykonawca w ofercie winny być parafowane przez osobę podpisującą ofertę.
8. Wykonawcy ponoszą wszelkie koszty związane z przygotowaniem i złożeniem oferty.
9. Oferty, których treść Wykonawca zmieni po upływie terminu składania ofert, Zamawiający odrzuci.
10. Wykonawca wskaże w formularzu oferty cenę za realizację całości przedmiotu zamówienia zgodnie z wyceną znajdującą się w formularzu oferty.
11. Walutą ceny oferty jest złoty polski. Zamawiający nie przewiduje stosowania walut obcych w rozliczeniu.
12. Wykonawca w formularzu ofertowym stanowiącym załącznik nr 1 do Zapytania ofertowego ustala całkowitą cenę oferty (cena brutto), która musi obejmować wszelkie obciążenia związane z realizacją przedmiotu zamówienia oraz wynikające z przepisów prawa, w tym wszelkie koszty, opłaty, wydatki Wykonawcy, a także podatki, w tym podatek od towarów i usług.
13. Cena musi uwzględniać wymagania niniejszego zapytania ofertowego, opisu przedmiotu zamówienia i istotnych postanowień umowy.
14. Wykonawca, dokonując kalkulacji warunków cenowych oferty, jest zobowiązany do przestrzegania zasad uczciwej konkurencji, z zastrzeżeniem, iż cena lub koszty lub ich istotne części składowe nie mogą być rażąco niskie w stosunku do przedmiotu zamówienia.
15. Wykonawca w przedstawionej ofercie winien zaoferować cenę kompletną jednoznaczną i ostateczną. Ewentualne upusty oferowane przez Wykonawcę winny być uwzględnione w cenie oferty.
16. Nie przewiduje się żadnych przedpłat ani zaliczek na poczet realizacji przedmiotu zamówienia, a płatność nastąpi zgodnie z zapisami Umowy.
17. Cena oferty powinna być podana z dokładnością do dwóch miejsc po przecinku, a zaokrąglenia należy wykonać zgodnie z zasadami matematycznymi (decyduje trzecia cyfra po przecinku, tj. jeśli trzecia cyfra mieści się w przedziale 0-4 – obowiązuje zaokrąglenie w dół, a jeśli mieści się w przedziale 5-9 – obowiązuje zaokrąglenie w górę).
18. Zamawiający nie dopuszcza składania ofert częściowych.
19. Termin związania ofertą wynosi 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
20. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą.
21. Tajemnica przedsiębiorstwa:
 - 1) Zamawiający informuje, że składane przez Wykonawców oferty są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj. Dz. U. z 2020 r. poz. 1913, z późn. zm.), jeśli Wykonawca w terminie składania ofert zastrzegł, że nie mogą być udostępniane i jednocześnie wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa (brak jednoznacznego wskazania, które



informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego zamówienia są jawne bez zastrzeżeń);

- 2) ujawnienie ofert odbywać się będzie wg poniższych zasad:
 - a) udostępnienie – po złożeniu wniosku (forma pisemna, elektroniczna lub faks) – należy podać informację o żądanym zakresie i formie udostępnienia dokumentów;
 - b) Zamawiający ustali, z uwzględnieniem złożonego w ofercie zastrzeżenia o tajemnicy przedsiębiorstwa, zakres informacji, które mogą być udostępnione;
 - c) Zamawiający wyznacza termin udostępnienia dokumentów, z uwzględnieniem czynności, o których mowa w lit. b);
- 3) w przypadku, gdy oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy, o której mowa w pkt 1), Wykonawca winien w sposób niebudzący wątpliwości zastrzec, które z zawartych w ofercie informacji stanowią tajemnicę przedsiębiorstwa i oznaczyć klauzulą: „DOKUMENTY ZASTRZEŻONE – TAJEMNICA PRZEDSIĘBIORSTWA”. Zaleca się wydzielenie tych informacji w złożonej ofercie. Wykonawca nie później niż w terminie składania ofert musi wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa;
- 4) Wykonawca nie może zastrzec informacji: nazwa (firma) oraz adres (siedziba) Wykonawcy, którego oferta jest otwierana, a także informacji dotyczących ceny oferty, terminu wykonania zamówienia, okresu gwarancji, warunków płatności zawartych w ofercie;
- 5) zastrzeżenie informacji, które nie stanowią tajemnicy przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji będzie traktowane, jako bezskuteczne i skutkować będzie ich odtajnieniem.

7. Termin i sposób składania ofert:

1. Ofertę należy złożyć w terminie **do dnia 8 lipca 2021 r.**
2. Ofertę wraz z dokumentami należy przesłać w formie elektronicznej na adres e-mail: ejadachowska@niw.gov.pl w temacie wiadomości wpisując: oferta - System Zarządzania Bezpieczeństwem Informacji

8. Ocena ofert:

1. Po upływie terminu wyznaczonego do składania ofert Zamawiający dokona ich analizy i oceny zgodnie z zasadami określonymi w niniejszym zapytaniu.
2. W toku badania i oceny ofert zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert lub uzupełnienia dokumentów wymaganych w zapytaniu.
3. Zamawiający poprawia w ofercie: oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, inne omyłki polegające na niezgodności oferty ze szczegółowymi informacjami dotyczącymi przedmiotu zamówienia niepowodujące istotnych zmian w treści oferty niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
4. W przypadku, gdy zaofferowana cena budzi wątpliwości Zamawiającego, co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w zapytaniu ofertowym, Zamawiający zwraca się o udzielenie wyjaśnień dotyczących wyliczenia ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny spoczywa na Wykonawcy.
5. Jeżeli nie można wybrać oferty z uwagi na fakt, dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów, zamawiający zaprasza Wykonawców, którzy złożyli oferty, do złożenia ofert



- dotychczasowych w wyznaczonym przez siebie terminie. Niedopuszczalne jest złożenie cen wyższych niż w złożonych ofertach.
6. W przypadku, gdy cena złożonych ofert przewyższa kwotę, którą Zamawiający może przeznaczyć na sfinansowanie zamówienia prowadzący postępowanie może zaprosić Wykonawców, którzy złożyli oferty, do złożenia ofert dodatkowych w wyznaczonym przez siebie terminie. Niedopuszczalne jest złożenie cen wyższych niż w złożonych ofertach.
 7. Zamawiający odrzuca ofertę jeżeli:
 - 1) Wykonawca, który złożył ofertę, zostanie wykluczony z postępowania;
 - 2) oferta została złożona po upływie terminu wyznaczonego na składanie ofert,
 - 3) jej treść nie odpowiada treści zapytania ofertowego;
 - 4) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
 - 5) Wykonawca nie udzielił wyjaśnień o których mowa w pkt. 4 lub jeżeli dokonana ocena wyjaśnień wraz ze złożonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia lub nie daje rękojmi należytego wykonania zamówienia;
 - 6) Wykonawca w terminie wyznaczonym nie zgodził się na poprawienie omyłki, o której mowa w pkt. 3;
 - 7) Wykonawca w terminie wskazanym przez Zamawiającego nie wyjaśnił wątpliwości bądź niejasności lub nie uzupełnił braków formalnych;
 - 8) Wykonawca nie wyraził zgody na przedłużenie terminu związania ofertą;
 - 9) jeżeli zawiera ona błędy w obliczeniu ceny niestanowiące omyłek rachunkowych;
 - 10) jest nieważna na podstawie powszechnie obowiązujących przepisów prawa;
 - 11) z innych uzasadnionych przyczyn, w szczególności gdy wykonawca podał nieprawdziwe lub wprowadzające w błąd dane, co mogło mieć wpływ na wynik postępowania.
 8. Zamawiający odrzuca ofertę Wykonawcy, który wcześniej wykonał nienależycie na rzecz Zamawiającego zamówienia publiczne w szczególności: nie wykonał zamówienia w umówionym terminie, nie dostarczył przedmiotu zamówienia o właściwej jakości i parametrach, nie wywiązał się w terminie z warunków gwarancji lub rękojmi, wykonał zamówienie, które było obciążone wadami powodującymi konieczność poniesienia dodatkowych nakładów finansowych lub prac przez Zamawiającego.
 9. Zamawiający informuje niezwłocznie Wykonawcę, którego oferta została odrzucona o powodach odrzucenia oferty podając uzasadnienie. Zawiadomienie to Zamawiający prześle na wskazany w ofercie adres e-mail. Odpowiedzialność za podanie niewłaściwego adresu e-mail ponosi Wykonawca.
 10. Z postępowania o udzielenie zamówienia wyklucza się Wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.
 11. Zamawiający informuje niezwłocznie Wykonawcę, który został wykluczony z postępowania, o powodach wykluczenia. Zawiadomienie to Zamawiający prześle na wskazany w ofercie adres e-mail. Odpowiedzialność za podanie niewłaściwego adresu e-mail ponosi Wykonawca.
 12. Za najkorzystniejszą uważa się ofertę (niepodlegającą odrzuceniu) z najniższą ceną.
 13. Zamawiający w każdej chwili może unieważnić postępowanie bez podania przyczyny.

9. Wykaz dokumentów, które należy złożyć wraz z ofertą:

Wraz z ofertą (załącznik nr 1 do Zapytania ofertowego) Wykonawca zobowiązany jest złożyć:

Wykaz usług (sporządzony wg. wzoru stanowiącego załącznik nr 3 do Zapytania ofertowego) na potwierdzenie spełniania warunków udziału w postępowaniu określonego w pkt 4.1.3) lit. a wraz z dokumentami potwierdzającymi należyte wykonanie (np. referencje, protokół odbioru).



Narodowy Instytut Wolności

Centrum Rozwoju Społeczeństwa Obywatelskiego

10. Wykaz załączników do zapytania ofertowego:

Załącznik nr 1 – formularz oferty

Załącznik nr 2 – istotne dla Stron postanowienia, które zostaną wprowadzone do treści umowy

Załącznik nr 3 – wykaz usług

Załącznik nr 4 – klauzula informacyjna