Somonino, 13.08.2025 r.

SE2.042.18.2024.WR

ZAPYTANIE OFERTOWE

Realizacja szkoleń i opracowanie dokumentacji w ramach projektu grantowego Cyberbezpieczny Samorząd – „Cyberbezpieczna Gmina Somonino”

Projekt realizowany w ramach Projektu Grantowego „Cyberbezpieczny Samorząd” realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy (FERC) 2021–2027, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa, finansowany z Europejskiego Funduszu Rozwoju Regionalnego (EFRR).
Tytuł projektu: „Cyberbezpieczna Gmina Somonino” Numer naboru: FERC.02.02-CS.01-001/23 Numer wniosku: 039c44e5-730f-47be-8039-6b7b2e0d2f37

W związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego o wartości nieprzekraczającej kwoty 130.000 zł zwracam się z prośbą o przedstawienie oferty cenowej wykonania zamówienia publicznego obejmującego:
Przedmiotem zamówienia jest opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnego z elementami normy ISO/IEC 27001, w celu zapewnienia zgodności z dyrektywą NIS2 oraz obowiązującymi przepisami prawa, a także przeprowadzenie szkoleń w ramach projektu „Cyberbezpieczny Samorząd” w Urzędzie Gminy Somonino oraz w jednej jednostce podległej — Gminnym Ośrodku Pomocy Społecznej w Somoninie.

W związku z projektem Cyberbezpieczny Samorząd i zawartą w ramach projektu umową o dofinansowanie Zamawiający zwraca się o złożenie oferty w przedmiocie ww. usługi.

Zamówienie realizowane będzie zgodnie z zasadami równości płci i dostępności dla osób z niepełnosprawnościami. Oferent zobowiązany jest do realizacji zamówienia zgodnie z Regulaminem Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” oraz zasadami określonymi w Programie Fundusze Europejskie na Rozwój Cyfrowy (FERC) 2021–2027 oraz z zasadami równości płci i dostępności dla osób z niepełnosprawnościami.
Projekt ma na celu podniesienie poziomu bezpieczeństwa informacji oraz spełnienie wymogów krajowego systemu cyberbezpieczeństwa w Urzędzie Gminy Somonino i Gminnym Ośrodku Pomocy Społecznej w Somoninie (GOPS).

I. Nazwa i adres Zamawiającego

GMINA SOMONINO
ul. Ceynowy 21
83-314 Somonino
NIP: 5891031191

II. Termin składania ofert:

Ostateczny termin składania oferty upływa 20.08.2025 r.

III. Miejsce i sposób składania ofert

Oferta powinna zostać przygotowana na formularzu oferty stanowiącym Załącznik nr 1 do Zapytania ofertowego. Oferty stanowiące odpowiedź na zapytanie wraz z załącznikami należy składać w formie:
1. pisemnej na adres: Urząd Gminy Somonino, ul. Ceynowy 21, 83-314 Somonino (decyduje data wpływu do Urzędu Gminy Somonino), lub
2. poprzez elektroniczną skrzynkę podawczą (epuap): /48c2g1mbx4/SkrytkaESP, lub
3. poprzez adres do e-Doręczeń Urzędu Gminy Somonino: AE:PL-56669-40373-RSUEF-29 lub
4. za pośrednictwem poczty elektronicznej (adres email): w.rolska@somonino.pl lub ug@somonino.pl

IV. Osoba uprawniona do kontaktu:

Weronika Rolska-Stencel tel. 58 743 23 54, adres e-mail: w.rolska@somonino.pl
Patryk Richert tel. 58 743 23 43, adres e-mail: p.richert@somonino.pl

V. Przedmiot zamówienia

Przedmiotem zamówienia jest:
1. Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji - Zakres i Etapy Wdrożenia SZBI
2. Szkolenia dotyczące bezpieczeństwa informacji w jednostkach dla pracowników i kadry kierowniczej.
3. Szkolenia specjalistyczne dla Informatyka, w zakresie zastosowania środków bezpieczeństwa

Szczegółowy opis przedmiotu zamówienia:

1. Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji Zakres i Etapy Wdrożenia SZBI

Wszystkie dokumenty projektowe — w tym dokumentacja SZBI, raporty audytów — muszą być opatrzone pełnokolorowym zestawem logotypów: Fundusze Europejskie, Rzeczpospolita Polska, Unia Europejska – Fundusze Europejskie — zgodnie z „Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich 2021–2027 w zakresie informacji i promocji".

1.1. **Audyt Wstępny:**
Wykonawca przeprowadzi dwa audyty wstępne – osobno dla Urzędu Gminy Somonino oraz dla Gminnego Ośrodka Pomocy Społecznej w Somoninie (GOPS), których celem będzie ocena aktualnego stanu systemu bezpieczeństwa informacji w dwóch jednostkach: Urzędzie Gminy Somonino oraz gminnym Ośrodku Pomocy Społecznej.

1.1.1. Konsultacje: Wykonawca zorganizuje spotkania z zespołem odpowiedzialnym za wdrożenie SZBI w obu jednostkach (po jednym spotkaniu w Urzędzie Gminy i GOPS) celem omówienia przeprowadzenia audytu wstępnego oraz przedstawienia procesu działania i planowanych do podjęcia działań i etapów audytu – narada wstępna.
1.1.2. Ocena zgodności z wymaganiami § 20 ust. 2 rozporządzenia KRI oraz normą ISO/IEC 27001, aby sprawdzić aktualny stan bezpieczeństwa informacji w obu jednostkach.

1.1.3. Analiza zabezpieczeń: Przeprowadzenie szczegółowej analizy zabezpieczeń systemów IT, identyfikacja luk w zabezpieczeniach oraz przedstawienie rekomendacji działań naprawczych dla Urzędu Gminy oraz GOPS.
1.1.4. Sporządzenie raportu z audytu wstępnego: Raport powinien zawierać szczegółowe wyniki analizy stanu systemu bezpieczeństwa informacji, z uwzględnieniem rekomendacji działań naprawczych i doskonalących.
1.1.5. Konsultacje: Wykonawca zorganizuje spotkania z zespołem odpowiedzialnym za wdrożenie SZBI w obu jednostkach (po jednym spotkaniu w Urzędzie Gminy i GOPS) celem omówienia wyników audytu wstępnego oraz przedstawienia zaleceń i planu działań naprawczych – narada zamykająca.
1.1.6. Podpisanie raportu przez audytorów: Raporty z audytu wstępnego muszą być podpisane przez audytorów, którzy przeprowadzili ocenę.

1.2. **Opracowanie Polityk i Procedur SZBI:**
Wykonawca opracuje i wdroży niezbędne polityki oraz procedury SZBI zgodne z wymaganiami normy ISO/IEC 27001 oraz przepisami krajowymi.

1.2.1. Polityka bezpieczeństwa informacji: Opracowanie polityki bezpieczeństwa informacji, która będzie zgodna z normą ISO/IEC 27001 oraz wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa. Polityki mają zostać przygotowane jako oddzielne dokumenty dla dwóch jednostek Urzędu Gminy oraz dla GOPS.
1.2.2. Cele i zakres SZBI: Zdefiniowanie celów i zakresu SZBI na podstawie analizy kontekstu organizacji, uwzględniając specyficzne zagrożenia i ryzyka, które mogą wystąpić w Urzędzie Gminy oraz GOPS. Dokumenty mają zostać opracowane oddzielnie dla dwóch jednostek Urzędu Gminy oraz dla GOPS.
1.2.3. Procedury zarządzania incydentami: Opracowanie procedur reagowania na incydenty związane z bezpieczeństwem informacji, w tym zasady postępowania w przypadku naruszenia ochrony danych.
1.2.4. System zarządzania dostępami: Opracowanie systemu zarządzania dostępem, kontrola uprawnień użytkowników oraz wdrożenie ścisłych procedur kontrolujących dostęp do systemów IT i danych w obu jednostkach.
1.2.5. Plan ciągłości działania (BCP) oraz plan reagowania na incydenty: Opracowanie dokumentów określających procedury zapewnienia ciągłości działania w przypadku awarii, jak i reagowania na incydenty związane z cyberbezpieczeństwem.
1.2.6. Ocena zgodności wdrożonych procedur: Analiza i ocena zgodności opracowanych polityk i procedur z normą ISO/IEC 27001 oraz przepisami prawa krajowego, ze szczególnym uwzględnieniem ustawy o krajowym systemie cyberbezpieczeństwa oraz regulacji NIS2.
1.2.7. Wsparcie w implementacji technicznych środków ochrony: Wykonawca dostarczy wsparcie w implementacji technicznych rozwiązań ochrony danych, takich jak szyfrowanie danych, systemy dwuskładnikowego uwierzytelniania, segmentacja sieci.
1.2.8. Opracowanie dokumentacji systemowej: Wykonawca opracuje pełną dokumentację systemu zarządzania bezpieczeństwem informacji, instrukcje operacyjne oraz polityki wewnętrzne dotyczące cyberbezpieczeństwa.
1.2.9. Dostosowanie dokumentacji do specyfiki jednostek, w ścisłej współpracy z zespołem odpowiedzialnym za wdrożenie SZBI w Urzędzie Gminy i GOPS.
1.2.10. Dostosowanie procedur do realiów organizacyjnych: Wdrażane procedury muszą być praktyczne, spójne z codziennym funkcjonowaniem organizacji oraz zapewniać zgodność z KRI oraz normą ISO 27001.

1.3. **Audyt Końcowy:**

Po wdrożeniu SZBI, Wykonawca przeprowadzi dwa audyty końcowe – po jednym dla Urzędu Gminy Somonino oraz Gminnego Ośrodka Pomocy Społecznej w Somoninie (GOPS). Audyty te będą miały na celu ocenę zgodności wdrożonego systemu zarządzania bezpieczeństwem informacji z normą ISO/IEC 27001 oraz wymaganiami obowiązujących przepisów prawa.

1.3.1. Ocena zgodności z wymaganiami § 20 ust. 2 rozporządzenia KRI oraz normą ISO/IEC 27001 po zakończeniu wdrożenia SZBI.
1.3.2. Analiza zabezpieczeń: Wykonawca przeprowadzi szczegółową analizę zabezpieczeń po wdrożeniu SZBI, identyfikując luki oraz przedstawiając rekomendacje działań naprawczych.
1.3.3. Sporządzenie raportu z audytu końcowego: Raport z audytu końcowego będzie zawierał wyniki analizy, wskazówki dotyczące dalszego doskonalenia systemu oraz rekomendacje naprawcze.
1.3.4. Podpisanie raportu przez audytorów: Raport z audytu końcowego musi być podpisany przez audytorów przeprowadzających ocenę.
1.3.5. Analiza punktów normy ISO 27001: Wykonawca przeanalizuje szczegółowo każdy punkt normy ISO 27001 w odniesieniu do wyników audytu wstępnego oraz oceni aktualny stan wdrożenia wymagań normy w jednostkach.
1.3.6. Dostosowanie procedur do realiów organizacyjnych: Wdrażane procedury muszą być praktyczne, spójne z codziennym funkcjonowaniem organizacji oraz zapewniać zgodność z KRI oraz normą ISO 27001.

1.4. **Opracowanie Dokumentacji:**
Wykonawca zobowiązany jest do opracowania pełnej odrębnej dla każdej jednostki dokumentacji wymaganej do certyfikacji SZBI zgodnie z normą ISO/IEC 27001, przygotowanej w formie umożliwiającej przekazanie dokumentów jednostce certyfikującej przez Zamawiającego. Dokumentacja ma być w formie wzorów i szablonów z możliwością implementacji przez Zmawiającego celem przeprowadzenia certyfikacji.

1.4.1. Dokumenty wymagane do certyfikacji: Wykonawca opracuje wszystkie dokumenty niezbędne do uzyskania certyfikacji zgodności z normą ISO/IEC 27001, w tym m.in. Księgę Systemu Zarządzania Bezpieczeństwem Informacji, Politykę Bezpieczeństwa Informacji, Plan Kontynuacji Działania (BCP), procedury audytu wewnętrznego, zarządzania incydentami, bezpieczeństwa fizycznego, procedurę nadzoru nad dokumentami, itp.
1.4.2. Wykonawca gwarantuje, że dokumentacja systemu zarządzania bezpieczeństwem informacji jest zgodna z wymaganiami normy ISO/IEC 27001 oraz wymagania certyfikacyjnymi jednostki certyfikującej systemy zarządzania na zgodność z normą ISO/IEC 27001, akredytowanej przez dowolną jednostką akredytującą wymienioną na stronie http://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4 .):

- Zakres systemu zarządzania bezpieczeństwem informacji
- Księga systemu zarządzania bezpieczeństwem informacji
- Polityka bezpieczeństwa informacji
- Polityka kontroli dostępu – czy istnieje polityka kontroli dostępu i czy podlega okresowym przeglądom i aktualizacjom
- Dostęp do sieci i usług sieciowych - czy wdrożone są narzędzia kontrolujące dostęp użytkowników wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia

- Rejestrowanie i wyrejestrowanie użytkowników – czy wdrożony jest formalny proces rejestrowania i wyrejestrowywania użytkowników
- Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników – czy istnieje formalny proces przydzielania poufnych informacji uwierzytelniających
- Przegląd praw dostępu – czy dokonywane są przeglądy praw dostępu użytkowników
- Odbieranie lub dostosowywanie praw dostępu – czy wdrożony jest formalny proces odbierania prawa dostępu do informacji i środków przetwarzania informacji po zakończeniu zatrudnienia lub dostosowania do zachodzących zmian w zatrudnieniu
- Schemat organizacyjny kierowania sprawami bezpieczeństwa informacji
- Deklaracja stosowania dla systemu bezpieczeństwa informacji
- Plan kontynuacji działania (BCP)
- Metodyka szacowania ryzyka

1.4.3. Wszystkie procedury potrzebne do przejścia procesu certyfikacji m.in.:

- Procedura nadzoru nad dokumentami
- Procedura działań korekcyjnych, korygujących i zapobiegawczych
- Procedura audytu wewnętrznego
- Procedura przeglądu zarządzania
- Procedura zarządzania incydentami
- Procedura bezpieczeństwa wewnętrznego organizacji
- Procedura ewakuacji personelu i sprzętu z obiektów
- Procedura klasyfikacji informacji wewnętrznych i zewnętrznych
- Procedura oceny ryzyk generowanych przez strony zewnętrzne (klientów, dostawców, kooperantów, innych)
- Procedura postępowania w przypadku odejścia pracownika z firmy
- Procedura bezpieczeństwa infrastruktury teleinformatycznej (sieć, serwerownie, urządzenia łączności, inne elementy)
- Procedura bezpieczeństwa fizycznego
- Procedura nadzór nad przyrządami pomiarowymi i zapewnienia spójności pomiarowej
- Inne niezbędne u klienta z punktu widzenia systemu bezpieczeństwa informacji (po ocenie potrzeb)
- Dokumenty ustalające status systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy.
- Opracowanie formularzy i rejestrów będących integralną częścią w/w dokumentów w formie i treści odpowiedniej do potrzeb i woli klienta.

1.5. **Analiza Ryzyka:**
W ramach analizy ryzyka, wykonawca przeprowadzi kompleksową ocenę ryzyka, uwzględniając aktywa, zagrożenia i podatności w obu jednostkach.

1.5.1. Identyfikacja aktywów i ocena ryzyka: Identyfikacja aktywów informacyjnych, technologicznych i ludzkich w obu jednostkach oraz ocena ryzyka związanego z ich utratą.

1.5.2. Ocena skutków utraty poufności, integralności i dostępności: Ocena skutków utraty poufności, integralności oraz dostępności dla kluczowych zasobów i aktywów organizacji.

1.5.3. Metodyka oceny ryzyka: Wykonawca zastosuje odpowiednią metodykę oceny ryzyka, identyfikując zagrożenia, podatności oraz określając działania naprawcze w celu minimalizacji ryzyk związanych z bezpieczeństwem informacji.

2. Szkolenia dotyczące bezpieczeństwa informacji w jednostkach dla pracowników i kadry kierowniczej.

Przedmiotem zamówienia jest przeprowadzenie szkoleń dla pracowników Urzędu Gminy (UG) oraz Gminnego Ośrodka Pomocy Społecznej (GOPS) w zakresie bezpieczeństwa informacji. Szkolenia będą obejmować tematykę z zakresu cyberbezpieczeństwa, regulacji wewnętrznych, wymagań rozporządzenia KRI oraz zasad bezpiecznego korzystania z Internetu. Program szkolenia musi uwzględniać specyfikę każdej jednostki i kłaść nacisk na praktyczne zastosowanie procedur bezpieczeństwa w codziennej pracy.

2.1. Wymagania Ogólne

2.1.1. Szkolenia muszą odbywać się w godzinach pracy Urzędu oraz jednostek organizacyjnych, przy czym dla pracowników Urzędu Gminy powinny odbywać się w godzinach pracy Urzędu, natomiast dla pracowników Gminnego Ośrodka Pomocy Społecznej – w godzinach pracy GOPS. Ze względu na planowane nieobecności pracowników wynikające z sezonu urlopowego w lipcu i sierpniu, szkolenie powinno zostać zrealizowane z wyłączeniem tych miesięcy.

2.1.2. Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia, i dostarczy go w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji Zamawiającego.

2.1.3. Opracowane materiały będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści. W ramach wynagrodzenia Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający dopuszcza dostarczenie kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF. Wszystkie materiały szkoleniowe pozostaną na stałe w zasobach Urzędu oraz GOPS, z możliwością ich dalszego wykorzystania do celów edukacyjnych i informacyjnych.

2.1.4. Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia.

2.1.5. Terminy szkoleń muszą być każdorazowo ustalane i zatwierdzane przez Zamawiającego przed ich realizacją.

2.1.6. Szkolenia powinny być prowadzone w formie stacjonarnej na terenie Gminy Somonino w miejscu wskazanym przez Zamawiającego.

2.1.7. Każdy uczestnik szkolenia otrzyma:

- Po zakończeniu każdego szkolenia, uczestnicy otrzymają imienny certyfikat ukończenia szkolenia, podpisany przez trenera. Ponadto certyfikat musi posiadać informacje: „Szkolenie zrealizowane w ramach projektu Cyberbezpieczna Gmina Somonino, dofinansowanego z Funduszy Europejskich w ramach programu Cyberbezpieczny Samorząd.” oraz musi być opatrzony pełnokolorowym zestawem logotypów: Funduszy Europejskich, Rzeczypospolitej Polskiej i Unii Europejskiej – zgodnie z „Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich 2021–2027 w zakresie informacji i promocji”.
- Materiały szkoleniowe oraz certyfikaty ukończenia szkoleń muszą być opatrzone zestawem logotypów: Fundusze Europejskie, Rzeczpospolita Polska, Unia Europejska – Fundusze Europejskie — zgodnie z wytycznymi „Podręcznika wnioskodawcy i beneficjenta Funduszy Europejskich 2021–2027 w zakresie informacji i promocji.

2.2. **Szczegółowy zakres szkolenia**

2.2.1. **Szkolenie dla pracowników i kadry kierowniczej – Moduł I (6 godzin), które ma zostać przeprowadzone przed audytem początkowym i rozpoczęciem wdrożenia. Szkolenie będzie wspólne tematycznie dla obu jednostek, jednak ze względu na organizację pracy powinno zostać zrealizowane osobno dla dwóch grup, w różnych terminach. Każda grupa będzie liczyć do 30 osób.**

2.2.1.1. Wprowadzenie do cyberbezpieczeństwa - znaczenie ochrony informacji w administracji publicznej.

- Definicja cyberbezpieczeństwa i jego znaczenie w organizacjach publicznych.
- Rola ochrony informacji w organizacji oraz zagrożenia związane z nieprzestrzeganiem zasad bezpieczeństwa informacji.

2.2.1.2. Podstawowe pojęcia związane z cyberbezpieczeństwem

- Omówienie terminologii: dane osobowe, dane wrażliwe, atak hakerski, cyberzagrożenia, phishing, vishing, itp.
- Definicje, znaczenie i praktyczne zastosowanie pojęć w kontekście bezpieczeństwa informacji w jednostkach publicznych.

2.2.1.3. Największe wycieki danych – przykłady

- Omówienie realnych przypadków wycieków danych i ich konsekwencji dla organizacji i osób fizycznych.
- Analiza przypadków dotyczących wycieków w sektorze publicznym.

2.2.1.4. Kary za naruszenia ochrony danych

- Omówienie przepisów prawnych, w tym RODO, oraz sankcji za nieprzestrzeganie zasad ochrony danych.

2.2.1.5. Rozpoznawanie zagrożeń i ataków socjotechnicznych

- Identyfikacja zagrożeń związanych z manipulacjami ludzkimi, takich jak phishing, vishing, baiting.
- Omówienie metod socjotechnicznych wykorzystywanych do pozyskania danych osobowych i informacji poufnych.
- Praktyczne przykłady ataków oraz sposoby skutecznej ochrony przed nimi.

2.2.1.6. Szyfrowanie, przechowywanie i udostępnianie danych

- Zasady bezpiecznego przechowywania danych, szyfrowania oraz metod ich udostępniania zgodnie z przepisami.

2.2.1.7. Zasady korzystania z poczty elektronicznej

- Bezpieczne korzystanie z poczty elektronicznej, ochronę przed spamem, phishingiem, zagrożeniami związanymi z załącznikami i linkami.

2.2.1.8. Bezpieczeństwo w Internecie

- Zasady bezpiecznego korzystania z przeglądarek internetowych, rozpoznawanie niebezpiecznych stron i ochrona prywatności.

2.2.1.9. Ochrona danych w chmurze

- Zasady przechowywania danych w chmurze oraz zabezpieczanie dostępu do nich, w tym szyfrowanie.

2.2.1.10. Bezpieczeństwo pracy zdalnej

- Zasady pracy zdalnej na sprzęcie służbowym i prywatnym, używanie VPN, zabezpieczenie urządzeń, unikanie publicznych sieci Wi-Fi.

2.2.1.11. Fake news i dezinformacja

- Jak rozpoznawać i przeciwdziałać dezinformacji oraz fake newsom w środowisku zawodowym.

2.2.1.12. Opracowanie i wdrożenie SZBI

- Kluczowe elementy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI): polityka bezpieczeństwa, procedury, zarządzanie ryzykiem.
- Etapy wdrożenia SZBI, monitorowanie i doskonalenie systemu.

2.2.1.13. Podsumowanie

- Podsumowanie kluczowych zagadnień szkolenia oraz praktyczne wskazówki wdrażania zasad bezpieczeństwa informacji.

2.3. **Szkolenie dla pracowników i kadry kierowniczej – Moduł II (6 godzin), które ma zostać przeprowadzone po wdrożeniu polityk oraz po zakończeniu audytu końcowego. Przewidziane są dwa oddzielne szkolenia, indywidualnie dopasowane do specyfiki każdej z jednostek.**

2.3.1. Dokumentacja SZBI w jednostce

- Przegląd wdrożonej dokumentacji SZBI w jednostkach oraz analiza praktycznych zastosowań.
- Zalecenia dotyczące szczególnych zagrożeń wynikających z specyfiki urzędów oraz konieczność dostosowania procedur.

2.3.2. Wykryte błędy w trakcie audytu wstępnego i audytu końcowego.

- Analiza wykrytych błędów oraz zalecenia audytowe.
- Proponowane działania w celu poprawy wdrożonych procedur.

2.3.3. Przedstawienie opracowanych procedur

- Omówienie zasad postępowania zgodnych z wdrożonym SZBI oraz ich wpływ na funkcjonowanie urzędu.
- Symulacje rzeczywistych sytuacji i ćwiczenia praktyczne w celu przetestowania skuteczności procedur.

2.4. **Szkolenie dla kadry kierowniczej (6 godzin) - Wspólne dla obu jednostek liczba uczestników do 15 os. odbywające się przed audytem początkowym i wdrożeniem.**

2.4.1. Omówienie NIS2 i polityki SZBI

- Przedstawienie wymagań wynikających z dyrektywy NIS2 oraz omówienie wdrożonej polityki SZBI w kontekście organizacyjnym i operacyjnym.
- Wskazanie odpowiedzialności kadry kierowniczej w zakresie zarządzania bezpieczeństwem informacji.

2.4.2. Określenie obowiązków wynikających z procedur

- Wyjaśnienie obowiązków pracowników w zakresie przestrzegania procedur, zarządzania dostępem do danych oraz reagowania na zagrożenia.

2.4.3. Wymagania normy ISO/IEC 27001, KRI oraz SZBI

- Przegląd wymagań normy ISO/IEC 27001 oraz KRI w kontekście organizacyjnym.
- Omówienie praktycznych aspektów wdrożenia SZBI oraz zarządzania bezpieczeństwem informacji w jednostkach publicznych.

2.4.4. Wymagania załącznika A normy ISO27001

- Szczegółowe omówienie wymagań zawartych w Załączniku A normy ISO 27001, w tym procedur oraz zasad bezpieczeństwa.

2.4.5. Szacowanie ryzyka

- Metody szacowania ryzyka w organizacji, identyfikacja ryzyk i propozycje działań zaradczych.
- Praktyczne przykłady obliczania ryzyka w kontekście bezpieczeństwa informacji.

2.4.6. Symulacje i ćwiczenia

- Realne przypadki oraz symulacje zagrożeń, które mogą wystąpić w pracy jednostki publicznej.

2.4.7. Podsumowanie i zalecenia

- Podsumowanie kluczowych zagadnień szkolenia, wskazówki dotyczące monitorowania i doskonalenia procedur bezpieczeństwa w jednostkach.

2.4.8. Forma szkolenia: Szkolenia będą odbywać się stacjonarnie, w siedzibach Zamawiającego (Urząd Gminy Somonino i GOPS Somonino).

2.4.9. Ilość uczestników:
Urząd Gminy Somonino do 47 os.
GOPS Somonino do 12 os.
Kadra Kierownicza: do 15 os.

2.5. **Szkolenia specjalistyczne dla Informatyka, w zakresie zastosowania środków bezpieczeństwa.**
Przedmiotem zamówienia jest przeprowadzenie szkoleń dla informatyka Urzędu Gminy (UG) w zakresie zastosowania środków bezpieczeństwa. Szkolenia będą obejmować tematykę z zakresu Cyberbezpieczeństwa. Szkolenia muszą odbywać się w godzinach pracy Urzędu.

2.5.1. **Wymagania ogólne**

2.5.1.1. Szkolenia powinny być prowadzone w formie stacjonarnej na terenie Gminy Somonino w miejscu wskazanym przez Zamawiającego. Zamawiający dopuszcza możliwość realizacji szkoleń w formie zdalnej (online).

2.5.1.2. Uczestnik szkolenia otrzyma:

- Po zakończeniu każdego szkolenia, uczestnik otrzyma imienny certyfikat ukończenia szkolenia, podpisany przez trenera. Ponadto certyfikat musi posiadać informacje: „Szkolenie zrealizowane w ramach projektu Cyberbezpieczna Gmina Somonino, dofinansowanego z Funduszy Europejskich w ramach programu Cyberbezpieczny Samorząd.” oraz musi być opatrzony pełnokolorowym zestawem logotypów: Funduszy Europejskich, Rzeczypospolitej Polskiej i Unii Europejskiej – zgodnie z „Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich 2021–2027 w zakresie informacji i promocji”.
- Materiały szkoleniowe oraz certyfikaty ukończenia szkoleń muszą być opatrzone zestawem logotypów: Fundusze Europejskie, Rzeczpospolita Polska, Unia Europejska – Fundusze Europejskie — zgodnie z wytycznymi „Podręcznika wnioskodawcy i beneficjenta Funduszy Europejskich 2021–2027 w zakresie informacji i promocji.

2.5.1.3. Terminy szkoleń muszą być każdorazowo ustalane i zatwierdzane przez Zamawiającego przed ich realizacją.

2.5.2. **Szczegółowy zakres szkolenia:**

2.5.2.1. **Szkolenie z zakresu administracji Proxmox VE i Proxmox Backup**

3. Czym jest Proxmox VE – rola i możliwości
4. Architektura i komponenty: KVM, LXC, QEMU, Ceph
5. Proxmox VE vs VMware ESXi vs Hyper-V vs XCP-ng
6. Model licencjonowania, wsparcie, społeczność
7. Wymagania sprzętowe i sieciowe
8. Instalacja z ISO lub migracja z Debian
9. Podstawowa konfiguracja: sieć, repozytoria, storage
10. Konfiguracja bridge, VLAN, Bonding
11. Tworzenie kontenerów LXC i maszyn KVM (VM)

11.1.1.1. Zarządzanie środowiskiem Proxmox

- Interfejs WebGUI, CLI, konsola Shell
- Zarządzanie dyskami i przestrzenią danych (ZFS, LVM, Ceph, NFS, CIFS)
- Snapshoty, migracje na żywo (live migration), klonowanie
- Monitorowanie zasobów, logów i użytkowników
- Ustawienia HA i klastra – podstawy

11.1.1.2. Proxmox Backup Server

- Czym jest PBS i jak działa (deduplikacja, szyfrowanie, kompresja)
- Architektura i różnice względem VZDUMP
- Instalacja PBS (bare-metal / VM)
- Dodawanie klienta backupu (Proxmox VE client)
- Konfiguracja backupów (zdalnych/lokalnych), harmonogramy
- Weryfikacja integralności backupu, rotacje, prunes

11.1.2. **Szkolenie z zakresu administracji i konfiguracji FortiGate oraz FortiMail**

11.1.2.1. Moduł 1: Wprowadzenie do FortiGate i architektury systemu

- Rola FortiGate jako NGFW (Next-Generation Firewall) i UTM
- Architektura FortiOS – funkcje systemu i ich moduły
- Tryby pracy FortiGate:
- NAT Mode vs Transparent Mode
- Integracja jako firewall brzegowy / wewnętrzny / SD-WAN
- Przegląd sprzętu i wersji wirtualnych FortiGate VM
- Licencjonowanie i aktualizacje systemu FortiOS

11.1.2.2. Moduł 2: Instalacja i podstawowa konfiguracja urządzenia

- Pierwsza konfiguracja GUI / CLI (console, SSH, web)
- Konfiguracja interfejsów sieciowych (Static / DHCP / PPPoE)
- Ustawienia DNS, NTP i synchronizacja czasu
- Zarządzanie użytkownikami i rolami administratora
- Tworzenie kopii zapasowych konfiguracji (TFTP, USB, cloud)
- Przywracanie systemu po awarii – factory reset, firmware recovery
- Diagnostyka CLI: get system status, diag sys top, diag sys session list

11.1.2.3. Moduł 3: Konfiguracja firewall i polityk bezpieczeństwa

- Polityki Firewall Policy
- Omówienie Implicit Deny
- Tworzenie reguł dostępu (IPv4, IPv6)
- Wdrożenie Deep Packet Inspection (DPI)
- NAT w FortiGate
- Source NAT (SNAT) – dynamiczny, statyczny
- Destination NAT (DNAT) – Virtual IP (VIP)
- Policy-Based NAT vs Central NAT
- Traffic Shaping (QoS) – priorytetyzacja ruchu

11.1.2.4. Moduł 4: Ochrona UTM – IPS, Web Filtering, AV, SSL Inspection

- IPS – Intrusion Prevention System:
- Tworzenie IPS Profiles
- Wykrywanie exploitów i blokowanie ataków
- Filtracja treści Web Filtering:

- Blokowanie stron (blacklist, whitelist)
- SSL Deep Inspection – inspekcja ruchu HTTPS
- Kontrola aplikacji (Application Control):
- Blokowanie ruchu P2P, VPN, TOR
- Kategoryzacja aplikacji (YouTube, Social Media)
- Antywirus i Anti-Botnet:
- Skanowanie AV w czasie rzeczywistym
- Blokowanie ruchu C2 (Command & Control)

11.1.2.5. Moduł 5: Konfiguracja VPN IPSec Site-to-Site i SSL VPN

- IPSec Site-to-Site:
- Konfiguracja tuneli IKEv1 vs IKEv2
- NAT Traversal, Dead Peer Detection (DPD)
- Troubleshooting (diagnose debug application ike)
- SSL VPN dla użytkowników zdalnych:
- Konfiguracja SSL VPN Portal
- Web Mode vs Tunnel Mode
- Integracja z LDAP, RADIUS, 2FA

11.1.2.6. Moduł 6: Routing i SD-WAN

- Routing statyczny vs dynamiczny:
- OSPF, BGP, ECMP
- Diagnostyka tras (get router info routing-table)
- SD-WAN – optymalizacja połączeń:
- Tworzenie reguł SLA
- Inteligentne przekierowanie ruchu
- Diagnostyka SD-WAN (diagnose sys sdwan)

11.1.2.7. Moduł 7: Zaawansowane mechanizmy bezpieczeństwa

- Role-Based Access Control (RBAC) – zarządzanie administratorami
- Integracja z Active Directory / LDAP
- Uwierzytelnianie wieloskładnikowe (2FA) – FortiToken

11.1.2.8. Moduł 8: Monitorowanie i diagnostyka FortiGate

- Analiza logów systemowych (Log & Report)
- Syslog i SNMP Monitoring
- Packet Capture i analiza ruchu (Wireshark, FortiGate PCAP)
- Debugowanie ruchu sieciowego:
- diagnose debug flow
- diag sys session list
- diag hardware sysinfo

11.1.2.9. Moduł 9: Optymalizacja i zabezpieczenie systemu

- Hardening systemu FortiOS:
- Minimalizacja powierzchni ataku
- Blokowanie nieużywanych usług
- Ograniczanie dostępu administracyjnego
- Zarządzanie aktualizacjami i podatnościami:
- Patch management dla FortiOS
- Automatyczne aktualizacje sygnatur IPS/AV

11.1.3. **Szkolenie Monitoring bezpieczeństwa z WAZUH i Elastic Stack**

11.1.3.1. Wersja: Darmowa, open-source (WAZUH Community + Elastic Open)

- Zrozumienie architektury WAZUH i Elastic Stack
- Instalacja i konfiguracja środowiska SIEM na własnej infrastrukturze (lokalnie lub w chmurze)
- Budowa centralnego systemu logowania i detekcji zagrożeń
- Tworzenie dashboardów, alertów i automatyzacja reakcji
- Symulacja analizy incydentów bezpieczeństwa

11.1.3.2. Moduł 1: Wprowadzenie do SIEM i WAZUH

- Czym jest SIEM? (Security Information and Event Management)
- Rola WAZUH w ekosystemie bezpieczeństwa
- Porównanie: WAZUH vs OSSEC vs komercyjne SIEM-y
- Omówienie przypadków użycia (compliance, SOC, DevSecOps)

11.1.3.3. Moduł 2: Architektura WAZUH i Elastic Stack

- Komponenty WAZUH: Wazuh Manager, Wazuh Agent, Filebeat / Auditbeat, Wazuh API, Integracja z Elastic Stack (Elasticsearch + Kibana)
- Komponenty Elastic: Elasticsearch – silnik analityczny, Kibana – dashboardy, wizualizacje, Beats (Filebeat, Auditbeat)
- Sposoby wdrożenia: lokalnie, chmura, Docker, Kubernetes

11.1.3.4. Moduł 3: Instalacja i konfiguracja

- Przygotowanie systemu (Linux / Windows / chmura)
- Instalacja Elastic Stack (Open Source): Elasticsearch + Kibana
- Instalacja WAZUH Manager
- Instalacja WAZUH Agent na różnych systemach (Linux, Windows)
- Instalacja Filebeat i integracja z Elastic

11.1.3.5. Moduł 4: Monitoring i zbieranie danych

- Konfiguracja agentów: FIM (File Integrity Monitoring), Rootcheck (wykrywanie rootkitów), Syscheck (zmiany w plikach), Sysmon + Winlogbeat (Windows Events), Logi aplikacji i systemu (syslog, journald, nginx, apache)
- Integracja z OSQuery (zapytania systemowe na żywo)
- Integracja z Auditd (Linux audit framework)

11.1.3.6. Moduł 5: Analiza danych i wizualizacja w Kibana

- Przegląd Dashboardów WAZUH w Kibanie
- Analiza zdarzeń: filtrowanie, korelacje, tagowanie
- Wizualizacje: wykresy, tabele, mapa geolokalizacji IP
- Tworzenie własnych dashboardów (np. dla logów nginx)

11.1.3.7. Moduł 6: Utrzymanie, hardening, bezpieczeństwo

- Aktualizacje i backupy WAZUH
- Bezpieczeństwo komunikacji (TLS)
- Hardening WAZUH i Elastic Stack
- Wydajność, skalowanie i monitoring infrastruktury

11.1.4. **Szkolenie administrowanie serwerami Windows - Windows Admin Center (WAC), powershell, SCCM.**

11.1.4.1. Nowe podejście Microsoft do zarządzania infrastrukturą serwerową

- Porównanie narzędzi: MMC, Server Manager, WAC, PowerShell, SCCM

- Przegląd architektury Windows Server 2019 / 2022
- Best practices zarządzania serwerami w środowiskach hybrydowych
- Instalacja i konfiguracja Windows Admin Center
- Dodawanie serwerów i klastrów do konsoli WAC
- Zarządzanie aktualizacjami, rolami i usługami
- Monitoring zasobów, logów zdarzeń i wydajności
- Zarządzanie lokalnie i zdalnie (Edge/Chrome, certyfikaty HTTPS)

11.1.4.2. PowerShell dla administratorów systemów

- Podstawy składni PowerShell (PS 5.1 vs 7.x)
- Wbudowane cmdlety dla Windows Server (Get-Service, Get-EventLog, Set-Item itp.)
- Zarządzanie użytkownikami, grupami, serwerami, usługami
- Tworzenie skryptów automatyzujących codzienne zadania (backup, restart usług, raportowanie)
- Praca z plikami CSV, logami i harmonogramem zadań
- Architektura System Center Configuration Manager
- Wymagania i komponenty: Site Server, Management Point, Distribution Point
- Zarządzanie urządzeniami: discovery, kolekcje
- Deployment systemów operacyjnych i aplikacji (overview)
- Aktualizacje systemowe (WSUS + SCCM), compliance i raportowanie
- Integracja z Intune i zarządzanie hybrydowe

12. Harmonogram Prac – Wdrożenie SZBI i Szkolenia w Gminie Somonino

12.1. Faza 1: Szkolenie Wstępne (Przed wdrożeniem SZBI)

- Moduł I dla Pracowników i Kadry Kierowniczej (UG i GOPS) - dwie grupy
- Szkolenie dla Kadry Kierowniczej (wspólne dla obu jednostek)

12.2. Faza 2: Audyt Wstępny i Planowanie SZBI:

- Konsultacje wstępne (UG i GOPS)
- Ocena zgodności (UG i GOPS)
- Analiza zabezpieczeń IT (UG i GOPS)
- Raport z audytu wstępnego
- Konsultacje zamykające (UG i GOPS)
- Podpisanie raportu

12.3. Faza 3: Opracowanie i Wdrożenie Dokumentacji SZBI

- Opracowanie polityk i procedur (UG i GOPS - oddzielnie)
- Wsparcie w implementacji zabezpieczeń
- Opracowanie dokumentacji systemowej
- Dostosowanie do specyfiki i realiów organizacji

12.4. Faza 4: Opracowanie Dokumentacji Certyfikacyjnej

- Opracowanie dokumentów do certyfikacji (UG i GOPS - oddzielnie)
- Gwarancja zgodności z normami i wymaganiami

12.5. Faza 5: Szkolenia Uzupełniające po Wdrożeniu SZBI

- Moduł II dla Pracowników i Kadry Kierowniczej (UG i GOPS) – osobno

12.6. Faza 6: Audyt Końcowy SZBI

- Ocena zgodności po wdrożeniu
- Analiza zabezpieczeń po wdrożeniu

- Raport z audytu końcowego
- Analiza ISO 27001
- Dostosowanie procedur

12.7. Szkolenia Specjalistyczne dla Informatyka – dowolnie w uzgodnieniu z Zamawiającym

- Administracja Proxmox VE i Backup
- Administracja i konfiguracja FortiGate i FortiMail
- Monitoring bezpieczeństwa z WAZUH i Elastic Stack
- Administrowanie serwerami Windows (WAC, PowerShell, SCCM)

Kody CPV:

79417000-0 – Usługi doradcze w zakresie bezpieczeństwa
72221000-0 – Usługi doradcze w zakresie analiz biznesowych
72225000-8 – Usługi doradcze w zakresie strategicznego przeglądu systemów informatycznych
80510000-2 – Usługi szkolenia specjalistycznego

Zapytanie prowadzone zgodnie z Wytycznymi w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2021-2027 oraz zgodnie z Zarządzeniem Nr 18/2021 Wójta Gminy Somonino z dnia 10 lutego 2021 roku, w sprawie wprowadzenia Regulaminu udzielania zamówień publicznych w Urzędzie Gminy Somonino, których wartość nie przekracza kwoty 130 000 zł.

VI. Termin realizacji zamówienia:

Zamówienie należy zrealizować w terminie do 17 listopada 2025 r. od dnia podpisania umowy.

VII. Warunki udziału w postępowaniu

O zamówienie mogą ubiegać się wykonawcy, którzy spełniają następujące warunki.

W zakresie dysponowania odpowiednim potencjałem kadrowym, Wykonawca zobowiązany jest wykazać, że skieruje do realizacji zamówienia niżej wymienione osoby, co umożliwi realizację zamówienia na odpowiednim poziomie jakości:

1. Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji - Zakres i Etapy Wdrożenia SZBI

a) co najmniej 1 osobą, która posiada certyfikat bezpieczeństwa systemów informatycznych (CISSP lub certyfikat równoważny w zakresie merytorycznym),
b) co najmniej 1 osobą, która posiada certyfikat bezpieczeństwa systemów informatycznych (CEH lub certyfikat równoważny w zakresie merytorycznym),
c) co najmniej 1 osobą, która posiada ukończony kurs dla audytora systemu zarządzania bezpieczeństwem informacji/audytora wiodącego (ISO 27001:2022 lub certyfikat równoważny w zakresie merytorycznym),
d) co najmniej 1 osobą, która posiada certyfikat audytora wiodącego ISO 22301:2019 lub certyfikat równoważny w zakresie merytorycznym,
e) co najmniej 1 osobę, która posiada certyfikat dotyczący audytu wewnętrznego Certified Internal Auditor (CIA) lub certyfikat równoważny w zakresie merytorycznym.

UWAGA:

Zamawiający dopuszcza możliwość łączenia potencjału kadrowego tzn. aby 1 osoba posiadała ww. certyfikaty.
Przez „certyfikat równoważny" należy rozumieć certyfikat potwierdzający kwalifikacje odpowiadające wymaganiom certyfikatu wskazanego powyżej, w szczególności w zakresie programu szkolenia, efektów kształcenia oraz wymagań egzaminacyjnych. Ocena równoważności będzie dokonywana przez Zamawiającego na podstawie dowodów przedstawionych przez Wykonawcę.

1. Szkolenia dotyczące bezpieczeństwa informacji w jednostkach dla pracowników i kadry kierowniczej oraz Szkolenia specjalistyczne dla Informatyka, w zakresie zastosowania środków bezpieczeństwa.

a) co najmniej 1 osobą, która posiada certyfikat bezpieczeństwa systemów informatycznych (CISSP lub certyfikat równoważny w zakresie merytorycznym),
b) co najmniej 1 osobą, która posiada certyfikat bezpieczeństwa systemów informatycznych (CEH lub certyfikat równoważny w zakresie merytorycznym),
c) co najmniej 1 osobą, która posiada ukończony kurs dla audytora systemu zarządzania bezpieczeństwem informacji/audytora wiodącego (IEC 27001:2005 lub certyfikat równoważny w zakresie merytorycznym),
d) co najmniej 1 osobą, która posiada certyfikat audytora ISO 22301:2019 lub certyfikat równoważny w zakresie merytorycznym.

UWAGA:
Zamawiający dopuszcza możliwość łączenia potencjału kadrowego tzn. aby 1 osoba posiadała ww. certyfikaty.
Przez „certyfikat równoważny" należy rozumieć certyfikat potwierdzający kwalifikacje odpowiadające wymaganiom certyfikatu wskazanego powyżej, w szczególności w zakresie programu szkolenia, efektów kształcenia oraz wymagań egzaminacyjnych. Ocena równoważności będzie dokonywana przez Zamawiającego na podstawie dowodów przedstawionych przez Wykonawcę.

Wykonawca ubiegający się o zamówienie wykaże się min. 2 letnim doświadczeniem w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.

VIII. Warunki wykluczenia z udziału w postępowaniu

Z udziału w postępowaniu są wykluczeni Wykonawcy, którzy:

1. Nie spełniają warunków udziału w postępowaniu umieszczonych w zapytaniu ofertowym, które są wskazane w Roz. VII zapytania bądź też nie dołączyli niezbędnych dokumentów potwierdzających spełnienie ww. warunków.
2. Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2024 r.,poz. 507).

IX. Kryteriami oceny ofert w niniejszym zapytaniu ofertowym są:

Cena, waga kryterium 100 %

X. Sposób przygotowania oferty

1. Ofertę należy sporządzić w języku polskim na załączonym druku „FORMULARZ OFERTY" (załącznik Nr 1 do zapytania ofertowego) wraz z oświadczeniem

stanowiącymi załącznik nr 2 oraz wykaz osób stanowiący załącznik nr 3 oraz wykaz usług stanowiący załącznik nr 4.

2. Zamawiający informuje, że jako jednostka samorządu terytorialnego jest zwolniony z podatku VAT w przypadku usług szkoleniowych zgodnie z art. 43 ust. 1 pkt 29 lit. c ustawy o podatku od towarów i usług (Dz. U. z 2024 r., poz. 361 z późn. zm.). W związku z tym Wykonawca powinien przygotować ofertę cenową z uwzględnieniem zwolnienia z VAT dla części dotyczącej szkoleń.
3. Cena ofertowa musi uwzględniać wszystkie koszty związane z realizacją zamówienia, zgodnie z opisem przedmiotu zamówienia oraz postanowieniami umowy, łącznie z pochodnymi z wynagrodzenia obciążającymi Zamawiającego.
4. Oferta Wykonawców wspólnie ubiegających się o zamówienie musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie (przez każdego z Wykonawców lub pełnomocnika).
5. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, dokumenty dotyczące przesłanek wykluczenia z postępowania musi złożyć każdy z Wykonawców składających ofertę wspólną; dokumenty dot. spełniania warunków udziału składa podmiot, który w odniesieniu do danego warunku udziału w postępowaniu potwierdza jego spełnianie.
6. Oferta powinna być przygotowana z uwzględnieniem poniższych zasad:

   a) Treść oferty musi odpowiadać treści zapytania ofertowego.
   b) Ofertę należy sporządzić w języku polskim.
   c) Oferta musi być złożona przez osobę uprawnioną do jej złożenia

7. Oferty niezgodne z ww. zasadami zostaną odrzucone.
8. Jeżeli zaoferowana cena lub koszt wydają się rażąco niskie w stosunku do przedmiotu zamówienia, tj. różnią się o więcej niż 30% od średniej arytmetycznej cen wszystkich ważnych ofert niepodlegających odrzuceniu, lub budzą wątpliwości zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w zapytaniu ofertowym lub wynikającymi z odrębnych przepisów, zamawiający żąda od wykonawcy złożenia w wyznaczonym terminie wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu. Zamawiający ocenia te wyjaśnienia w konsultacji z wykonawcą i może odrzucić tę ofertę wyłącznie w przypadku, gdy złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej ceny lub kosztu w tej ofercie.
9. Zapytanie ofertowe może być unieważnione przez Zamawiającego bez podania przyczyny w każdym momencie.
10. Zamawiający wezwie wykonawcę do wyjaśnienia lub uzupełniania dokumentów składanych w odpowiedzi na zapytanie.

Załączniki:

1. Załącznik nr 1 - Formularz oferty
2. Załącznik nr 2 - Oświadczenie o spełnianiu warunków i nie podleganiu wykluczeniu
3. Załącznik nr 3 - Oświadczenie o braku okoliczności wskazanych w art. 7 ust. 1 ustawy o przeciwdziałaniu wspieraniu agresji na Ukrainę
4. Załącznik nr 4 – Oświadczenie o braku powiązań osobowych i kapitałowych
5. Załącznik nr 5 - Wykaz osób
6. Załącznik nr 6 – Wykaz usług
7. Załącznik nr 7 - Wzór umowy
8. Załącznik nr 8 – Zobowiązanie innego podmiotu

Administratorem danych osobowych jest Wójt Gminy Somonino.
Oferent ma prawo żądać od Administratora dostępu, sprostowania, usunięcia, ograniczenia, przeniesienia swoich danych osobowych, wniesienia sprzeciwu oraz skargi do organu nadzorczego, chyba, że realizacja tych praw nie jest zgodna z przepisami prawa. Szczegółowe informacje dotyczące procesu przetwarzania danych osobowych przez Wójta Gminy Somonino dostępne są w siedzibie Urzędu Gminy w Somoninie oraz na stronie internetowej http://bip.somonino.pl/

Z up.
Wójta Gminy Somonino
Zastępca Wójta Gminy Somonino
Andrzej Peta

Andrzej Peta
Elektronicznie podpisany przez Andrzej Peta
Data: 2025.08.13 16:31:17 +02'00'