Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID – 19

Łowicz, dn. 24 czerwca 2022 r.

ZAPYTANIE OFERTOWE

I. Znak Sprawy: I.271.4.5.2022.DF

II. Zamawiający

Gmina Miasto Łowicz
Stary Rynek 1
99-400 Łowicz
NIP 834-18-82-502
REGON 750148621

III. Tryb udzielania zamówienia publicznego

Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie zapytania ofertowego wyłączonego z obowiązku stosowania ustawy z dnia 11.09.2019 r. - Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 z późn. zm.), o którym mowa w art. 2 ust. 1 pkt 1).

Informacje ogólne

Zamawiający:
Urząd Miejski w Łowiczu
Pl. Stary Rynek 1
99-400 Łowicz
telefon: 46 830 91 51-52
Internet: http://www.lowicz.eu/bip/
Adres do korespondencji:
Urząd Miejski w Łowiczu
Pl. Stary Rynek 1
99-400 Łowicz
telefon: (46) 830 91 23 (osoby wyznaczone do kontaktu)

Data publikacji:	**27 czerwca 2022 r.**
Termin składania oferty:	**11 lipca 2022 r.**
Termin zadawania pytań do zapytania:	**4 lipca 2022 r.**

Opis przedmiotu zamówienia publicznego

Nazwa zamówienia:

Audyt cyberbezpieczeństwa

Rodzaj i przedmiot zamówienia zgodnie ze Wspólnym Słownikiem Zamówień CPV

Główny CPV

72810000 Usługi audytu komputerowego

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest przeprowadzenie audytu wewnętrznego bezpieczeństwa informacji w siedzibie zamawiającego, zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. 2017 poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI. w tym opracowanie raportu zawierającego wnioski i rekomendacje.
W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do:

1. **Przeprowadzenia audytu bezpieczeństwa danych w systemach informatycznych oraz sieci ICT:**

1.1 Analiza wszystkich zabezpieczeń przed utratą i kradzieżą danych
1.2 Analiza kontroli dostępu do systemów informatycznych w tym dostępu przez usługi i narzędzia zdalne
1.3 Analiza zabezpieczeń przy pracy zdalnej
1.4 Analiza i ocena technicznej infrastruktury w systemach ICT, schematu sieci a także technicznych zabezpieczeń sieci.
1.5 Analiza i ocena zabezpieczeń dostępu do sieci publicznej
1.6 Analiza i ocena zabezpieczeń wewnętrznej sieci ICT
1.7 Ocena sposobu identyfikowania i logowania użytkowników
1.8 Analiza i ocena systemów backupów i archiwizacji danych w tym testy odtworzeniowe.
1.9 Analiza i ocena ciągłości pracy systemów i sieci ICT
1.10 Testy penetracyjne systemów informatycznych i całej infrastruktury ICT
1.11 Sprawdzenie zabezpieczeń komputerów przed atakami phishingowymi
1.12 Badanie podatności usług sieciowych
1.13 Badanie podatności aplikacji serwera pocztowego email i aplikacji webowej zgodnie z OWASP.
1.14 Weryfikacja systemu uwierzytelniania użytkowników i administratorów
1.15 Weryfikacja systemu uwierzytelniania użytkowników i administratorów do systemu operacyjnego i kontrolera domeny
1.16 Sprawdzenie sposobów i systemów szyfrowania.
1.17 Sprawdzenie systemów ochrony poczty email i usług WEB pod kątem ataków phishingowych
1.18 Analiza i ocena sposobu zbierania logów, zakresu i retencji logów
1.19 Identyfikacja pojedynczych punktów awarii

2. **Przeprowadzenia audytu danych zgodnie z przepisami RODO, UODO, KRI, KSC**

2.1 Analiza zgodności dokumentacji ochrony danych osobowych
2.2 Analiza upoważnień do przetwarzania danych osobowych

2.3 Analiza umów powierzenia przetwarzania danych osobowych
2.4 Analiza umów i porozumień dotyczących przekazywania danych osobowych
2.5 Analiza rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania
2.6 Ocena procesu zarządzania incydentami i reagowania na incydenty. Analiza informacji lub raportów dotyczących, incydentów naruszenia bezpieczeństwa danych
2.7 Analiza konieczności dokonania oceny skutków dla planowanych sposobów przetwarzania danych
2.8 Rozpoznanie roli i funkcji IODO
2.9 Kontrola zabezpieczeń zbiorów tradycyjnych
2.10 Kontrola zabezpieczeń zbiorów archiwalnych
2.11 Kontrola systemu monitoringu
2.12 Kontrola systemu alarmowego
2.13 Weryfikacja kontroli nad przepływem danych osobowych
2.14 Weryfikacja poufności, dostępności i udostępniania danych osobowych
2.15 Analiza i ocena zagrożeń z identyfikacją słabych stron związanych z przetwarzaniem danych
2.16 Weryfikacja dostępu osób nieupoważnionych do miejsc, gdzie przetwarzane są dane
2.17 Analiza i ocena procedur zarządzania systemami teleinformatycznymi
2.18 Analiza i ocena zaangażowania Najwyższego Kierownictwa w proces ciągłego doskonalenia systemu bezpieczeństwa informacji
2.19 Analiza i ocena ochrony ICT przed oprogramowaniem szkodliwym, w tym weryfikacja zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
2.20 Analiza i ocena procedur historii zmian w dokumentach, systemach informatycznych itp.
2.21 Analiza i ocena procedur zarządzania i zabezpieczania nośników przechowujących dane
2.22 Analiza i ocena zasad odpowiedzialności użytkowników
2.23 Analiza i ocena zasad zarządzania hasłami
2.24 Analiza i ocena zabezpieczeń kryptograficznych
2.25 Analiza i ocena zabezpieczeń komputerów przenośnych w tym praca zdalna.
2.26 Analiza stopnia zabezpieczenia stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe
2.27 Analiza i ocena niszczenia niepotrzebnych nośników oraz danych

3. Opracowania raportu zawierającego ocenę stosowanych zabezpieczeń, analizę stanu bezpieczeństwa, wnioski, zalecenia i rekomendację dotyczące zakresu, metodyki i organizacji zabezpieczeń

4. **Diagnoza cyberbezpieczeństwa** Diagnoza cyberbezpieczeństwa (audyt) musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. 2017 poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI

4.2 Diagnoza musi zostać wykonana zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina] - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.

4.3 Audyt musi zostać przeprowadzony przez osobę posiadającą co najmniej jedno z uprawnień wykazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu:
   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 (Dz. U. z 2022 r. poz. 5), w zakresie certyfikacji osób
d) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 2230 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

5. Zamawiający wymaga, aby audyt był przeprowadzony w siedzibie Zamawiającego.
6. Wymagany termin realizacji zamówienia:
   Wykonawca jest zobowiązany wykonać zamówienie nie później niż w terminie 60 dni od dnia zawarcia umowy.

Wynikiem audytu musi być:

1. pełny raport z przeprowadzonego audytu
2. wypełniony formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa zamieszczony na stronach Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina] - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8
3. rekomendacje dotyczące technicznych zabezpieczeń danych i informacji

Wszystkie dokumenty wynikowe powinny być sporządzone w formie papierowe – 2 egzemplarze oraz elektronicznej w formacie docx.

Szczegółowe parametry zamówienia:

n)	Ilość pracowników	98
o)	Ilość lokalizacji	4
p)	Ilość serwerów fizycznych	8
q)	Ilość serwerów wirtualnych	10
r)	Ilość macierzy	4
s)	Ilość drukarek sieciowych	37
t)	Ilość stacji komputerowych	83

u)	Ilość laptopów	29
v)	Ilość stacji obsługujących USC, DO i Ewidencję Ludności	9
w)	Ilość VLAN-ów	65
x)	Adresy zewnętrzne	15
y)	Access Point	13
z)	Active Directory.	Wdrożone

Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny ich spełniania

1) Z możliwości składania ofert wyklucza się Oferentów, którzy:

Są podmiotem powiązanym z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta 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, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. (Dz. U. z 13 kwietnia 2022 r. poz. 835) o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych wyklucza się:

a) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
b) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie

decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;

c) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ppkt 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

2) W postępowaniu mogą wziąć udział podmioty, które wykażą, że wykonały w instytucjach administracji publicznej (w gminach) co najmniej 2 audyty cyberbezpieczeństwa

3) Dokumenty wymagane od wykonawcy
   a) formularz ofertowy
   b) dokument stwierdzający prawo osoby (osób) podpisującej ofertę do reprezentowania wykonawcy w postępowaniu o uzyskanie przedmiotowego zamówienia publicznego, w szczególności aktualny odpis z Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, pełnomocnictwo,
   c) na żądanie Zamawiającego, Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu zamieszcza informacje o podwykonawcach w oświadczeniach.
   d) dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu;
   e) referencje potwierdzające prawidłowe wykonanie audytu.

4) Zamawiający zastrzega możliwość sprawdzenia informacji zawartych w dokumentach.

Kryteria oceny oferty Informacja o wagach punktowych lub procentowych przypisanych do poszczególnych kryteriów oceny oferty

Zamawiający oceni i porówna jedynie te oferty, które nie zostaną odrzucone przez Zamawiającego. Oferty zostaną ocenione przez Zamawiającego w oparciu o następujące kryteria i ich znaczenie:

Kryterium	Znaczenie procentowe kryterium	Maksymalna liczba punktów, jakie może otrzymać oferta za dane kryterium
Cena brutto	100 %	100 pkt

Sfinansowano w ramach reakcji Unii na pandemię COVID – 19

Termin składania ofert

1. Podpisaną ofertę wraz z ww. załącznikami należy dostarczyć do siedziby Zamawiającego osobiście lub listem poleconym/kurierem do dnia **11 lipca 2022 r. do godz. 10:00.** Decyduje data faktycznego wpływu oferty do Zamawiającego (nie np. data nadania, data stempla pocztowego). Oferty, które wpłyną po terminie zostaną odrzucone. Opis na kopercie z ofertą:
   Audyt cyberbezpieczeństwa
   lub
   drogą elektroniczną w postaci zaszyfrowanej na skrytkę ePUAP adres:
   /lr24qxn733/SkrytkaESP
   do godz. **10:00 do dnia 11 lipca 2022 r.** r., hasło SMS-em na telefon 608667682 o godz. **10:00** w dniu **11 lipca 2022** r. – dokumenty elektroniczne muszą być podpisane podpisem kwalifikowanym przez osoby upoważnione.
   Oferty niekompletne lub niezgodne z warunkami udziału w postępowaniu, będą odrzucone.
2. Pytania do niniejszego zapytania należy kierować na adres e-mail: dariusz.fabijanski@um.lowicz.pl do dnia **4 lipca 2022 r.**r. Pytania zadane po tym terminie nie będą rozpatrywane.

Postanowienia dodatkowe i końcowe

1. Zamawiający zapłaci za faktycznie wykonaną usługę na podstawie faktury wystawionej przez Wykonawcę.
2. Zapłata zostanie dokonana w terminie do 30 dni po otrzymaniu poprawnie wystawionej faktury.
3. Wykonawca ponosi wszelkie koszty własne związane z przygotowaniem i złożeniem oferty, niezależnie od wyniku postępowania. Zamawiający nie odpowiada za koszty poniesione przez Wykonawcę w związku z przygotowaniem i złożeniem oferty.
4. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert.
5. Termin związania ofertą: 30 dni kalendarzowych.
6. Złożenie oferty jest jednoznaczne z zaakceptowaniem powyższych zasad.

W załączeniu:
1. Załącznik nr 1 – projekt umowy
2. Załącznik nr 2 – formularz ofertowy

Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID – 19

Klauzula informacyjna o przetwarzaniu danych osobowych

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. – dalej RODO uprzejmie informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Miasto Łowicz reprezentowane przez Burmistrza Miasta Łowicza, z siedzibą pod adresem: pl. Stary Rynek 1, 99-400 Łowicz.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się pod adresem e-mail: iod@um.lowicz.pl
3. Pani/Pana dane osobowe przetwarzane będą w celu przeprowadzenia zamówienia oraz zawarcia i realizacji umowy (w przypadku gdy oferta będzie najkorzystniejsza) na podstawie:
   - art. 6 ust. 1 lit. c RODO tj. w związku z wypełnieniem obowiązku prawnego ciążącego na Administratorze w celu związanym z prowadzeniem postępowania z wyłączeniem przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych w związku z przepisami ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
   - art. 6 ust. 1 lit. b RODO tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.
4. Z uwagi na możliwość współfinansowania zamówienia ze środków w ramach Programu Operacyjnego Polska Cyfrowa 2014 – 2020 (dalej: „POPC 2014 – 2020") odbiorcą Pani/Pana danych osobowych może być Instytucja Zarządzająca POPC. Informację o przetwarzaniu danych osobowych przez Instytucję Zarządzającą znajdzie Pan/Pani na stronie Internetowej: https://www.polskacyfrowa.gov.pl/strony/o-programie/zasady-przetwarzania-danych-osobowych-w-programie-polska-cyfrowa/
5. Odbiorcami Pani/Pana danych osobowych będą podmioty upoważnione na podstawie przepisów prawa lub wykonujące zadania realizowane w interesie publicznym, m.in. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o ustawę o dostępie do informacji publicznej z dnia 6 września 2001 r. oraz ustawę z dnia 27 sierpnia 2009 r. o finansach publicznych.
6. Pani/Pana dane osobowe pozyskane w związku z postępowaniem o udzielenie zamówienia publicznego – dokumentacja zamówień publicznych, przetwarzane będą w celach archiwalnych przez okres 5 lat. Dane osobowe, uzyskane w związku z umową zawartą w wyniku postępowania w trybie zamówień publicznych przetwarzane będą przez okres trwania umowy, a następne w celach archiwalnych przez okres 10 lat.
7. W przypadku współfinansowania zamówienia w ramach POPC 2014 – 2020, dane zostaną zarchiwizowane i będą przechowywane do czasu rozliczenia POPC 2014 – 2020.
8. Pani/Pana dane osobowe nie będą przekazywane do państw trzecich lub organizacji międzynarodowych.
9. Posiada Pani/Pan prawo żądania:
   - dostępu do treści swoich danych osobowych;
   - sprostowania swoich danych osobowych (*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)*;
   - usunięcia swoich danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
   - ograniczenia przetwarzania danych osobowych (*prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu ustalenia, dochodzenia lub obrony roszczeń*

lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);

10. Posiada Pani/Pan prawo do wniesienia skargi do organu nadzorczego (Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa).
11. Podanie danych jest dobrowolne, ale bez ich podania nie będzie możliwe wzięcie pod uwagę przedstawionej oferty oraz zawarcie i realizacja umowy, jeżeli oferta będzie najkorzystniejsza;
12. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą profilowane.

Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID – 19

Z up. BURMISTRZA
Dariusz Fabijański
Gł. Specjalista ds. Informatyki

Sporządził:

Dariusz Fabijański

Zatwierdzam:

Krzysztof Jan Kaliński

BURMISTRZ
Kaliński
Krzysztof Jan Kaliński