

ZAPYTANIE OFERTOWE

Powiat Wrocławski - Powiatowy Zakład Katastralny we Wrocławiu z siedzibą we Wrocławiu, 50-440 Wrocław, ul. Tadeusza Kościuszki 131, zaprasza do złożenia ofert na:

1. Przedmiot zamówienia:

„Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Powiatowego Zakładu Katastralnego we Wrocławiu.”

2. Termin zakończenia realizacji zamówienia: **do dnia 19 grudnia 2025 r.**

3. Ofertę należy sporządzić w języku polskim z zachowaniem formy pisemnej, na formularzu stanowiącym Załącznik nr 2 do Zapytania ofertowego – *Formularz oferty*, z uwzględnieniem następujących informacji:

- 1) nazwa i adres Wykonawcy;
- 2) dane kontaktowe Wykonawcy - numer telefonu i adres poczty elektronicznej (e-mail);
- 3) NIP i REGON Wykonawcy;
- 4) cena ofertowa całości przedmiotu zamówienia w PLN (złotych polskich) z rozbiciem na: cenę netto, podatek VAT oraz cenę brutto;
- 5) termin realizacji całości zamówienia;
- 6) warunki płatności;
- 7) inne istotne warunki wykonania zamówienia;

i akceptacją oświadczeń o:

- 1) zapoznaniu się z warunkami określonymi w Zapytaniu ofertowym, w tym z Projektem umowy i Opisem Przedmiotu Zamówienia oraz brakiem zastrzeżeń do ich treści;
- 2) pozyskaniu wszystkich niezbędnych informacji do przygotowania oferty;
- 3) zgodności składanej oferty z warunkami określonymi w Zapytaniu ofertowym;

i przekazać wraz z załącznikami:

- 1) aktualnym odpisem z właściwego rejestru lub CEiDG;
- 2) podpisanym oświadczeniem dot. przesłanek wykluczenia z 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 (Załącznik nr 4);
- 3) podpisanym oświadczeniem w zakresie wskazania Naczelnika Urzędu Skarbowego właściwego dla Wykonawcy (Załącznik nr 5);
- 4) podpisanym oświadczeniem o dysponowaniu zasobami osobowymi, które wykonają przedmiot zamówienia (Załącznik nr 6);
- 5) kopie (skan) certyfikatów uprawniających do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077), zgodnie z oświadczeniem, o którym mowa w pkt. 4.

4. Ofertę należy złożyć w terminie do dnia: **11 sierpnia 2025 r. do godz. 13:00**, w formie:

- 1) pisemnej (osobiście albo listownie) na adres: 50-440 Wrocław ul. T. Kościuszki 131;
- 2) lub faksem na numer: 71 372 43 47;
- 3) lub w wersji elektronicznej lub w formie dokumentacyjnej na adres poczty elektronicznej (e-mail): pzk@kataster.wroc.pl.

5. Oferta musi być podpisana przez osobę upoważnioną do składania ofert i podpisywania oświadczeń w postępowaniach o udzielenie zamówień publicznych.

6. Zamawiający odrzuci ofertę, która zostanie złożona po terminie, o którym mowa w pkt 7 niniejszego Zapytania.

7. Wykonawca jest związany ofertą przez okres 7 dni. Bieg terminu rozpoczyna się z upływem terminu składania ofert.

8. Realizacja zamówienia zostanie powierzona Wykonawcy, który przedłoży wszystkie dokumenty wymagane w Zapytaniu ofertowym oraz zaoferuje **najniższą cenę ofertową całości przedmiotu zamówienia**, jako jedyne

kryterium wyboru najkorzystniejszej oferty. Cena podana w ofercie musi uwzględniać wszystkie koszty związane z wykonaniem całości przedmiotu zamówienia.

9. Zamawiający zastrzega sobie możliwość dodatkowych negocjacji cen.
10. Podstawą do realizacji zamówienia będzie zawarcie umowy niezwłocznie po wyborze najkorzystniejszej oferty.
11. Zamawiający unieważni niniejsze zapytanie, jeżeli nie wpłynie żadna oferta.
12. Osoby upoważnione do kontaktu z Wykonawcami:
 - 1) Dominik Cichoń;
 - 2) Piotr Karcz– tel. 71 345 99 34; di@kataster.wroc.pl.
13. Klauzula informacyjna: 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 (Dz. Urz. UE L 119, dalej „RODO”), informuję że:
 - 1) administratorem Pana/Pani danych osobowych jest Powiatowy Zakład Katastralny we Wrocławiu, ul. T. Kościuszki 131, 50-440 Wrocław, tel. 71 372 40 08, pzk@kataster.wroc.pl;
 - 2) Inspektorem Ochrony Danych Osobowych jest Pani Małgorzata Czarторыska, tel. 519-375-959, rodo@kataster.wroc.pl;
 - 3) podstawa prawna przetwarzania – art. 6 ust. 1 pkt a RODO;
 - 4) cel przetwarzania danych osobowych – postępowanie o udzielenie zamówienia publicznego prowadzone w procedurze zapytania ofertowego;
 - 5) dane osobowe nie są udostępniane do państwa trzeciego lub organizacji narodowej;
 - 6) odbiorcami Pani/Pana danych osobowych będą: pracownicy Powiatowego Zakładu Katastralnego we Wrocławiu, organy kontrolne, osoby lub podmioty, którym Administrator udzielił informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 poz. 1764 ze zm.), ustawą z dnia 11 sierpnia 2021 r. o otwartych danych i o ponownym wykorzystaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524), podmioty przetwarzające dane osobowe w imieniu Administratora na mocy zawartych innych umów, inne podmioty upoważnione na podstawie przepisów prawa powszechnie obowiązującego;
 - 7) podane dane będą przetwarzane przez czas niezbędny do przeprowadzenia przedmiotowego postępowania, przygotowania, zawarcia i realizacji umowy;
 - 8) podanie przez Wykonawcę danych osobowych wynikających z zapisów zapytania ofertowego jest dobrowolne, jednakże odmowa ich podania jest równoznaczna z brakiem możliwości wyboru oferty Wykonawcy;
 - 9) posiada Pani/Pan prawo do sprostowania i dostępu do Pani/Pana danych osobowych oraz prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
 - 10) nie przysługuje Pani/Panu prawo do usunięcia danych osobowych, przenoszenia danych osobowych, o którym mowa w art. 20 RODO oraz prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. C RODO.
14. Załączniki do Zapytania ofertowego:
 - 1) Opis Przedmiotu Zamówienia – Załącznik nr 1;
 - 2) Formularz oferty – Załącznik nr 2;
 - 3) Projekt Umowy – Załącznik nr 3;
 - 4) Oświadczenie Wykonawcy dot. przesłanek wykluczenia z 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 – Załącznik nr 4;
 - 5) Oświadczenie w zakresie wskazania Naczelnika Urzędu Skarbowego właściwego dla Wykonawcy – Załącznik nr 5.
 - 6) Oświadczenie Wykonawcy w zakresie dysponowania zasobami osobowymi, które wykonają przedmiot zamówienia – Załącznik nr 6.



DYREKTOR

Justyna Skrzyńska-Nowak

(podpis osoby upoważnionej)

PZK-DA.G.222.55.2025

OPIS PRZEDMIOTU ZAMÓWIENIA
Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Powiatowego Zakładu Katastralnego we Wrocławiu

I. Cel zamówienia:

Celem zamówienia jest opracowanie kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Powiatowego Zakładu Katastralnego we Wrocławiu (dalej PZK) w oparciu o wymagania norm:

PN-EN ISO/IEC	pełny tytuł	zakres normy
27001:2023-08	Techniki informatyczne – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania	Określa wymagania dotyczące ustanowienia, wdrożenia, utrzymywania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w kontekście ryzyka biznesowego organizacji, zapewniając wybór odpowiednich środków ochrony informacji.
27002:2023-01	Techniki informatyczne – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji	Dostarcza praktyczne wskazówki dotyczące wyboru, wdrożenia i zarządzania środkami ochrony bezpieczeństwa informacji, w tym kontrolami bezpieczeństwa zgodnymi z załącznikiem A normy PN-EN ISO/IEC 27001, obejmującymi kontrole z zakresu ochrony fizycznej, logicznej, organizacyjnej oraz zasobów ludzkich.
27005:2025-01	Techniki informatyczne – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji	Obejmuje zasady oraz procesy identyfikacji, oceny, analizy, traktowania i monitorowania ryzyk związanych z bezpieczeństwem informacji w celu wspierania wymagań określonych w normie PN-EN ISO/IEC 27001.
22301:2020-04	Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania	Określa wymagania dotyczące planowania, ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia systemu zarządzania ciągłością działania, umożliwiającego organizacji przygotowanie się na zakłócenia, reagowanie na nie oraz odzyskiwanie po nich w celu ograniczenia skutków incydentów.

dostosowanej do specyfiki jednostki sektora finansów publicznych (JST), z uwzględnieniem przepisów krajowych i unijnych w zakresie ochrony informacji, cyberbezpieczeństwa oraz przetwarzania danych osobowych. Dokumentacja wraz ze szkoleniami ma stanowić podstawę do wdrożenia systemu oraz przygotowanie jednostki do certyfikacji (opcjonalnej), a także zapewnić spełnienie obowiązków wynikających z obowiązujących przepisów prawa, w tym w szczególności:

- 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 uchyłające dyrektywę 95/46/WE* (ogólne rozporządzenie o ochronie danych).
- ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. z 2019 r. poz. 1781),
- ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2024 r. poz. 1077),
- ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2024 r. poz. 1557),

- rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999).

II. Zakres przedmiotu zamówienia:

1. Opracowanie szczegółowego harmonogramu realizacji zamówienia

- 1) W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest do opracowania szczegółowego harmonogramu realizacji wszystkich czynności niezbędnych do sporządzenia kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), którego celem jest uporządkowanie etapów przygotowania dokumentacji SZBI, transparentna kontrola przebiegu realizacji zamówienia, minimalizacja ryzyka opóźnień w przekazaniu dokumentacji, dostosowanie przebiegu realizacji do bieżącego funkcjonowania PZK bez zakłócania pracy jednostki.
- 2) Opracowanie harmonogramu musi uwzględniać:
 - a) ustalenie etapów realizacji zamówienia obejmuje:
 - etap przygotowawczy: analiza wstępna i audyt zerowy jednostki (przegląd stanu istniejącego, identyfikacja obszarów ryzyka, zidentyfikowanie brakujących procedur),
 - opracowanie pełnej dokumentacji SZBI (dokumentacja obowiązkowa i rekomendowana zgodna z PN-EN ISO/IEC 27001:2023-08, PN-EN ISO/IEC 27002:2023-01, PN-EN ISO/IEC 27005:2025-01, PN-EN ISO/IEC 22301:2020-04),
 - konsultacje robocze z Zamawiającym (przekazywanie projektów dokumentów, zbieranie uwag, wprowadzanie poprawek),
 - przeprowadzenie szkoleń dla pracowników,
 - przygotowanie raportu końcowego z audytu zerowego oraz protokołu przekazania dokumentacji SZBI;
 - b) określenie terminów realizacji poszczególnych etapów musi uwzględniać przewidywaną liczbę dni roboczych potrzebnych na:
 - przeprowadzenie analizy wstępnej i audytu zerowego,
 - opracowanie i przekazywanie projektów dokumentacji do weryfikacji przez Zamawiającego,
 - wprowadzenie uwag Zamawiającego oraz finalizację dokumentacji;
 - c) wskazanie osób odpowiedzialnych po stronie Wykonawcy za realizację poszczególnych etapów oraz danych kontaktowych do komunikacji roboczej;
 - d) określenie działań wymagających zaangażowania pracowników Zamawiającego, takich jak:
 - udostępnienie danych i dokumentów niezbędnych do analizy (np. procedury wewnętrzne, schematy organizacyjne, wykaz systemów informatycznych),
 - udział w spotkaniach konsultacyjnych w celu omówienia projektów dokumentacji,
 - wskazanie osób za kontakt z Wykonawcą;
 - e) możliwość monitorowania postępu realizacji przez Zamawiającego,
 - f) raportowanie postępu w formie mailowej oraz w ramach ustalonych spotkań roboczych (stacjonarnych lub online),
 - g) rezerwę czasową na wprowadzenie uwag Zamawiającego do dokumentacji przed jej finalnym przekazaniem.
- 3) Wykonawca jest zobligowany do przygotowania i przedłożenia Zamawiającemu harmonogramu do akceptacji, do 10 dni roboczych od podpisania Umowy.
- 4) Harmonogram stanowi podstawę do rozliczenia realizacji przedmiotu zamówienia i ewentualnego naliczania kar umownych, zgodnie z § 4 ust. 1 pkt 1 Umowy.

2. Analiza wstępna i audyt zerowy (przedwdrożeniowy)

- 1) Wykonawca w ramach realizacji zamówienia przeprowadzi szczegółową analizę wstępną oraz audyt zerowy w celu:
 - uzyskania pełnego obrazu stanu bezpieczeństwa informacji w PZK,
 - identyfikacji aktywów informacyjnych, procesów, zasobów i przepływów informacji,
 - opisu istniejących środków ochrony fizycznej, technicznej i organizacyjnej,
 - identyfikacji potencjalnych zagrożeń, podatności i niezgodności,
 - dokonania wstępnej oceny ryzyka (risk assessment),
 - opracowania zaleceń w zakresie dostosowania istniejącej dokumentacji do specyfiki jednostki, wymagań statutowych i przetwarzanych danych,
 - zapewnienia zgodności z obowiązującymi przepisami prawa i normami PN-EN ISO/IEC 27001:2023-08, PN-EN ISO/IEC 27002:2023-01, PN-EN ISO/IEC 27005:2025-01, PN-EN ISO/IEC 22301:2020-04.
- 2) Zakres działań:
 - a) zebranie danych i przygotowanie analizy, w tym w szczególności:
 - przeprowadzenie spotkania otwierającego z kierownictwem i osobami odpowiedzialnymi za obszary IT, kadry, administrację oraz ochronę danych osobowych (IOD),
 - przegląd dokumentów, w tym:
 - statutu i regulaminów regulujących organizację jednostki,
 - obowiązujących polityk i procedur (ochrona danych osobowych, systemy IT i in.),
 - wykazów użytkowników systemów informatycznych,
 - dokumentacji systemów informatycznych i systemów kadrowych/finansowych,
 - umów powierzenia przetwarzania danych osobowych i in. dokumentów niezbędnych do przygotowania dokumentacji SZBI,
 - b) identyfikacja aktywów informacyjnych - opracowanie wykazu aktywów informacyjnych, w tym:
 - dokumentacji analogowej (akta pracowników, dokumentacja geodezyjna, dokumentacja finansowo-księgowa itd.),
 - danych w systemach informatycznych (bazy danych, rejestry publiczne),
 - sprzętu komputerowego i serwerów,
 - aplikacji użytkowych,
 - danych osobowych przetwarzanych w PZK,
 - danych poufnych i danych wrażliwych, jeżeli są przetwarzane.
 - c) analiza przepływu informacji:
 - identyfikacja kluczowych procesów przetwarzania danych,
 - określenie przepływów danych między komórkami organizacyjnymi oraz podmiotami zewnętrznymi (urzędy, firmy serwisowe, wnioskodawcy, w tym wykonawcy geodezyjni itd.),
 - identyfikacja punktów newralgicznych w przepływie informacji, w tym przesyłania danych drogą elektroniczną i tradycyjną.
 - d) ocena stosowanych zabezpieczeń:
 - ocena zabezpieczeń fizycznych:
 - kontrola dostępu do pomieszczeń,
 - zabezpieczenia przeciwpożarowe,

- monitorowanie i ochrona obiektu.
- ocena zabezpieczeń technicznych:
 - zabezpieczenia systemów informatycznych (antywirusy, firewall, kopie zapasowe),
 - zabezpieczenia dostępu logicznego (hasła, uprawnienia użytkowników),
 - stosowanie szyfrowania nośników i transmisji danych.
- ocena zabezpieczeń organizacyjnych:
 - upoważnienia do przetwarzania danych osobowych,
 - procedury reagowania na incydenty oraz zagrożenia zewnętrzne,
 - szkolenia z zakresu bezpieczeństwa informacji.
- e) identyfikacja zagrożeń i podatności:
 - opracowanie listy potencjalnych zagrożeń dla aktywów informacyjnych (np. nieuprawniony dostęp, utrata danych, ataki zewnętrzne),
 - określenie podatności organizacyjnych i technicznych mogących wpływać na bezpieczeństwo informacji.
- f) wstępna ocena ryzyka:
 - przeprowadzenie uproszczonej analizy ryzyka metodą jakościową lub ilościową,
 - określenie obszarów ryzyka wymagających wdrożenia środków ochrony,
- g) opracowanie raportu z analizy wstępnej i audytu zerowego:
 - opis stanu istniejącego,
 - lista wykrytych niezgodności i obszarów do poprawy,
 - wstępna mapa ryzyk i rekomendacje dla SZBI,
 - wskazanie obszarów wymagających dodatkowej dokumentacji,
 - rekomendacje dotyczące szkoleń dla pracowników.
- 3) Przygotowanie analizy wstępnej i audytu zerowego będzie zrealizowane przez zespół pod kierunkiem specjalisty posiadającego certyfikaty określone w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999), uprawniające do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zgodnie ze złożonym Oświadczeniem w zakresie dysponowania zasobami osobowymi, które wykonają przedmiot zamówienia.
- 4) Dokument podsumowujący analizę wstępną i audyt zerowy będzie zawierał następujące informacje: stronę tytułową (nazwa raportu, wykonawca, data), cel i zakres analizy oraz audytu, metodyka audytu, wyniki analizy wstępnej i audytu, zidentyfikowane ryzyka, niezgodności oraz rekomendacje oraz załączniki (np. lista kontrolna, lista osób uczestniczących).
- 5) Termin realizacji analizy wstępnej i audytu zerowego zostanie określony w harmonogramie, o którym mowa w ust. 1.

3. Opracowanie dokumentacji SZBI

- 1) Wykonawca w ramach realizacji zamówienia opracuje kompletną dokumentację SZBI w celu:
 - przygotowania spójnego, dostosowanego do struktury i potrzeb PZK zestawu dokumentów zgodnych z wymaganiami norm PN-EN ISO/IEC 27001:2023-08, PN-EN ISO/IEC 27002:2023-01, PN-EN ISO/IEC 27005:2025-01, PN-EN ISO/IEC 22301:2020-04 oraz przepisami prawa (w tym RODO, KSC, NIS2, ustawą o informatyzacji), które umożliwią skuteczne zarządzanie bezpieczeństwem informacji w jednostce,

- ujednolicenia procedur postępowania w zakresie ochrony informacji, zapewniających odpowiednie zabezpieczenie danych przetwarzanych w PZK, w tym danych osobowych, rejestrów publicznych oraz danych istotnych dla działania jednostki,
 - utworzenia kompletnej dokumentacji obowiązkowej i rekomendowanej (m.in. polityka bezpieczeństwa informacji, procedury, instrukcje, rejestry, wzory upoważnień, matryce ryzyka), gotowej do wdrożenia w codziennym funkcjonowaniu jednostki,
 - spełnienia wymagań audytowych oraz umożliwienie ewentualnego przyszłego uzyskania certyfikacji zgodności z ISO/IEC 27001,
 - przygotowania PZK do działania zgodnie z zasadami ciągłości działania i ochrony zasobów informacyjnych, w celu minimalizacji ryzyk związanych z utratą poufności, dostępności oraz integralności informacji w jednostce.
- 2) Zakres dokumentacji wymaganej przez PN-EN ISO/IEC 27001:2023-08, PN-EN ISO/IEC 27002:2023-01, PN-EN ISO/IEC 27005:2025-01, PN-EN ISO/IEC 22301:2020-04 oraz zgodnej z najlepszymi praktykami JST i ISO musi obejmować co najmniej następujące zagadnienia:
- a) Polityka bezpieczeństwa informacji – dokument określający cele, zasady i podejście do bezpieczeństwa informacji w PZK, zgodny z norami PN-EN ISO/IEC 27001:2023-08, PN-EN ISO/IEC 27002:2023-01, PN-EN ISO/IEC 27005:2025-01, PN-EN ISO/IEC 22301:2020-04 oraz przepisami prawa,
 - b) cele SZBI i plan osiągnięcia celów – dokument wskazujący zidentyfikowane strony, wymagania prawne i regulacyjne,
 - c) zakres przedmiotowy, podmiotowy i terytorialny SZBI,
 - d) deklaracja stosowania (SoA) – identyfikacja, uzasadnienie i deklaracja zastosowania lub wyłączenia poszczególnych środków bezpieczeństwa (kontrolnych),
 - e) procedury SZBI, w tym co najmniej:
 - zarządzanie incydentami bezpieczeństwa informacji,
 - zarządzanie dostępem i nadawaniem uprawnień,
 - zarządzanie zasobami informacyjnymi,
 - zarządzanie kopiami zapasowymi,
 - zarządzanie zmianami,
 - postępowanie postępowania z incydentami,
 - postępowanie w przypadku naruszenia ochrony danych osobowych,
 - zarządzanie ryzykiem w obszarze bezpieczeństwa informacji, w tym metodologia szacowania ryzyka oraz plan postępowania z ryzykiem,
 - postępowanie w sytuacjach awaryjnych i przywracania po awarii (DRP)
 - procedury ciągłości działania (BCP),
 - bezpieczne użytkowanie urządzeń mobilnych i nośników danych.
 - f) rejestry wymagane przepisami i normą, w tym:
 - rejestr incydentów bezpieczeństwa,
 - rejestr aktywów informacyjnych, w tym zasobów informacyjnych i systemów IT,
 - rejestr ryzyk w obszarze bezpieczeństwa informacji,
 - rejestr naruszeń ochrony danych osobowych,
 - rejestr szkoleń z zakresu bezpieczeństwa,

- g) instrukcje wewnętrzne wspierające politykę SZBI, w tym m.in. instrukcja zarządzania systemami informatycznymi (zgodna z RCI), instrukcja zarządzania hasłami, instrukcja klasyfikacji informacji, instrukcja postępowania z nośnikami danych,
 - h) wzory upoważnień i oświadczeń dotyczących zachowania poufności oraz wzory umów powierzenia przetwarzania danych,
 - i) matryce ról i odpowiedzialności w zakresie SZBI,
 - j) wzór raportu z audytu wewnętrznego oraz plan audytu wewnętrznego.
- 3) Opracowanie dokumentacji SZBI będzie zrealizowane przez zespół pod kierunkiem specjalisty posiadającego certyfikaty określone w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. *w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu* (Dz. U. z 2018 r. poz. 1999), uprawniające do przeprowadzania audytu w rozumieniu art. 15 *ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, zgodnie ze złożonym *Oświadczeniem w zakresie dysponowania zasobami osobowymi, które wykonają przedmiot zamówienia*.

4. Przeprowadzenie szkolenia dla pracowników PZK:

- 1) Wykonawca w ramach realizacji zamówienia zobowiązany jest do przeprowadzenia szkoleń, które są kluczowym elementem wdrażania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
- 2) Szkolenia mają na celu:
 - a) zwiększenie świadomości pracowników poprzez:
 - zapoznanie pracowników z podstawowymi zasadami bezpieczeństwa informacji,
 - uświadomienie roli każdego pracownika w ochronie danych, w tym danych osobowych oraz innych danych chronionych,
 - rozumienie zagrożeń związanych z naruszeniem poufności, integralności i dostępności danych,
 - b) zapoznanie z politykami i procedurami SZBI:
 - przekazanie wiedzy o nowo opracowanych politykach SZBI i obowiązujących procedurach (np. klasyfikacja danych, postępowanie w przypadku incydentu, zarządzanie dostępami),
 - wyjaśnienie obowiązków pracowników wynikających z przepisów prawa (RODO, KSC, NIS2, ustawa o informatyzacji) i przepisów wewnętrznych PZK,
 - c) zapewnienie zgodności z wymaganiami norm PN-EN ISO/IEC 27001:2023-08, PN-EN ISO/IEC 27002:2023-01, PN-EN ISO/IEC 27005:2025-01, PN-EN ISO/IEC 22301:2020-04, aby pracownicy byli świadomi polityki bezpieczeństwa informacji, celów SZBI oraz ich roli w osiągnięciu tych celów,
 - d) ograniczenie ryzyk wynikających z błędów ludzkich - zmniejszenie prawdopodobieństwa incydentów związanych z niewłaściwym przetwarzaniem informacji, np. przesyłaniem danych nieuprawnionym osobom, używaniem słabych haseł, czy otwieraniem podejrzanych załączników,
 - e) przygotowanie do reagowania na incydenty:
 - przekazanie zasad rozpoznawania i zgłaszania incydentów bezpieczeństwa zgodnie z procedurami SZBI w PZK,
 - wyjaśnienie podstawowych działań, jakie pracownicy powinni podejmować w przypadku stwierdzenia incydentu (np. wyciek danych, phishing, zgubienie nośnika),
 - f) wzmocnienie kultury bezpieczeństwa w PZK:
 - budowanie postawy odpowiedzialności za przetwarzane dane wśród wszystkich pracowników,
 - wskazanie korzyści płynących z przestrzegania zasad bezpieczeństwa zarówno dla jednostki, jak i samych pracowników;

- 3) Wykonawca zobowiązany jest do przeprowadzenia szkoleń:
- a) w podziale na minimum cztery grupy pracowników: kadra zarządzająca, pracownicy działu IT, pracownicy komórki finansowo-księgowej i administracyjnej, pozostali pracownicy PZK,
 - b) zakończonych testami wiedzy w podziale na specyfikę grup pracowników,
 - c) w łącznym wymiarze nie krótszym niż 28 roboczogodzin.

III. Produkty zamówienia:

- 1) Szczegółowy harmonogram realizacji zamówienia, o którym mowa w rozdz. II ust. 1:
 - format: .pdf oraz .docx,
 - liczba egzemplarzy papierowych: 2 egzemplarze,
 - termin przekazania określony, w rozdz. 2 ust. 1 pkt 3;
- 2) Raport z analizy wstępnej i audytu wewnętrznego, o których mowa w rozdz. II ust. 2
 - format: .pdf oraz .docx,
 - liczba egzemplarzy papierowych: 2 egzemplarze,
 - termin przekazania: zgodnie z harmonogramem;
- 3) Pełna dokumentacja SZBI, o której mowa w rozdz. II ust. 3:
 - format: .pdf oraz .docx,
 - dokumentacja powinna być spójna graficznie, opatrzona logiem PZK i logo wykonawcy w części raportowej,
 - liczba egzemplarzy papierowych: 3 egzemplarze,
 - termin przekazania: zgodnie z harmonogramem;
- 4) Potwierdzenie przeprowadzenia szkoleń, o których mowa w rozdz. II ust. 4
 - format: .pdf,
 - zawartość: lista obecności pracowników uczestniczących w szkoleniach, raport z przeprowadzonego szkolenia (tematyka, agenda, liczba uczestników, czas trwania), arkusze testów wiedzy lub raport z quizu online wraz z podsumowaniem wyników, potwierdzenie przeprowadzenia szkolenia podpisane przez wykonawcę i przedstawiciela Zamawiającego, o którym mowa w § 6 ust. 2 Umowy,
 - liczba egzemplarzy papierowych: 1 egzemplarz,
 - termin przekazania: niezwłocznie po przeprowadzeniu szkoleń, zgodnie z harmonogramem.
- 5) Uwagi szczegółowe w zakresie produktów zamówienia:
 - a) wszystkie produkty opracowania muszą zostać przekazane w wersji papierowej i elektronicznej w sposób umożliwiający ich archiwizację oraz praktyczne wykorzystanie przez Zamawiającego,
 - b) wersja elektroniczna powinna być przekazana w postaci jednego archiwum .zip, zawierającego pliki w formacie .pdf (wersja ostateczna, podpisana elektronicznie lub skan podpisanej wersji) oraz .docx (w celu umożliwienia późniejszych aktualizacji przez PZK),
 - c) wszystkie dokumenty muszą posiadać spis treści, numerację stron i wersjonowanie dokumentu (np. wersja 1.0, data),
 - d) dokumenty w wersji papierowej należy przekazać w segregatorach lub oprawionych w sposób umożliwiający ich archiwizację.



DYREKTOR
Justyna Skrzyńska-Nowak



PZK-DA.G.222.55.2025

.....
(miejscowość, data)

FORMULARZ OFERTY

Powiat Wrocławski
Powiatowy Zakład Katastralny
we Wrocławiu
ul. Kościuszki 131
50-440 Wrocław

Nazwa Wykonawcy:
Adres Wykonawcy:
nr tel. e-mail:
NIP: REGON:

Na podstawie uzyskanego Zapytania ofertowego podejmuję się wykonania przedmiotu zamówienia zgodnie z dobrą praktyką, wiedzą, obowiązującymi przepisami oraz należyłą starannością i składam ofertę w postępowaniu prowadzonym w trybie zapytania ofertowego zgodnie z ustawą z dnia 23 kwietnia 1964 r. *Kodeks cywilny* (t. j. Dz. U. z 2024 r. poz. 1061) na realizację zamówienia dotyczącego:

**„Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
dla Powiatowego Zakładu Katastralnego we Wrocławiu.”**

I. Cena ofertowa całości przedmiotu zamówienia (w PLN):

netto zł +% VAT zł

brutto zł

Powyższa cena zawiera wszystkie koszty związane z realizacją zamówienia.

II. Termin realizacji całości zamówienia: do 19 grudnia 2025 r.

III. Warunki płatności:

Wynagrodzenie płatne będzie przelewem, na wskazany przez Wykonawcę rachunek bankowy, w terminie do 21 dni od daty dostarczenia Zamawiającemu prawidłowo wystawionej faktury VAT.

IV. Inne istotne warunki wykonania zamówienia:

Jednocześnie:

- Oświadczam/y, że zapoznałem/liśmy się z warunkami określonymi w dokumentach *Zapytania ofertowego*, w tym z Projektem Umowy i Opiszem Przedmiotu Zamówienia, i nie wnoszę/simy do nich żadnych zastrzeżeń.
- Oświadczamy, że pozyskałem/liśmy wszystkie niezbędne informacje do przygotowania oferty, a przedłożona oferta jest zgodna z warunkami określonymi w dokumentach *Zapytania ofertowego*.

3. Do niniejszego *Formularza oferty* załączam/y:

- 1) aktualny odpis z właściwego rejestru lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEiDG), jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert
- 2) oświadczenie dot. przesłanek wykluczenia z 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 (*Załącznik nr 4 do Zapytania ofertowego*);
- 3) oświadczenie w zakresie wskazania Naczelnika Urzędu Skarbowego właściwego dla Wykonawcy (*Załącznik nr 5 do Zapytania ofertowego*);
- 4) oświadczenie Wykonawcy w zakresie dysponowania zasobami osobowymi, które wykonają przedmiot zamówienia (*Załącznik nr 6 do Zapytania ofertowego*);
- 5) kopie (skan) certyfikatów wymaganych w *Zapytaniu ofertowym* przez Zamawiającego.

.....
(pieczętka Wykonawcy)

.....
(czytelny podpis Wykonawcy)

PZK-DA.G.222.55.2025

UMOWA Nr /2025

zawarta we Wrocławiu w dniu złożenia przez Strony ostatniego kwalifikowanego podpisu elektronicznego pomiędzy:

Powiatem Wrocławskim - Powiatowym Zakładem Katastralnym we Wrocławiu
z siedzibą przy ul. T. Kościuszki 131, 50-440 Wrocław, NIP – 8971647961, BDO – 000519885,
reprezentowanym przez: Dyrektora – Panią Justynę Skrzynecką - Nowak,
zwanym dalej **Zamawiającym**,

a:

.....

z siedzibą przy ul.

REGON –, NIP -

reprezentowaną przez:

zwanym dalej **Wykonawcą**.

Niniejszą Umowę zawarto bez stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. 2024 r. poz. 1320 ze zm.), na podstawie art. 2 ust. 1 pkt 1 cytowanej ustawy oraz z zastosowaniem przepisów Regulaminu udzielania zamówień publicznych obowiązującego w Powiatowym Zakładzie Katastralnym we Wrocławiu.

§ 1

1. Zamawiający zleca a Wykonawca przyjmuje do wykonania:

Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Powiatowego Zakładu Katastralnego we Wrocławiu.

2. Szczegółowy zakres prac związany z realizacją usługi, o której mowa w ust. 1, został zawarty w Opisie Przedmiotu Zamówienia – Załącznik nr 1, który wraz z ofertą Wykonawcy – Załącznik nr 2 i Wykazem osób – Załącznik nr 3, stanowi integralną część Umowy.

§ 2

Wykonawca zobowiązuje się do wykonania usługi będącej przedmiotem zamówienia w terminie do dnia **19 grudnia 2025 r.**

§ 3

1. Wynagrodzenie za wykonanie zamówienia, o którym mowa w § 1 wynosi:

..... zł netto

+ VAT % tj. zł,

czyli łącznie brutto zł (słownie: zł 00/100).

2. Kwota określona w ust. 1 jest ceną ryczałtową i obejmuje wykonanie całości przedmiotu zamówienia, o którym mowa w § 1.

3. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszystkie koszty, związane z realizacją zamówienia.

4. Podstawą wystawienia faktury VAT będzie protokół odbioru podpisany przez obie strony.

5. Fakturę VAT należy wystawić na:

Nabywca: Powiat Wrocławski, ul. Tadeusza Kościuszki 131, 50-440 Wrocław, NIP: 8971647961

Odbiorca: Powiatowy Zakład Katastralny we Wrocławiu, ul. Tadeusza Kościuszki 131, 50-440 Wrocław.

6. Wynagrodzenie płatne będzie przelewem, na wskazany przez Wykonawcę rachunek bankowy, w terminie do 21 dni od daty dostarczenia Zamawiającemu prawidłowo wystawionej faktury VAT.
7. Datą zapłaty faktury VAT będzie data obciążenia konta Zamawiającego.
8. Numer rachunku rozliczeniowego wskazany w fakturze VAT wystawionej w ramach Umowy, należy do Wykonawcy i jest rachunkiem, dla którego zgodnie z rozdz. 3a ustawy z dnia 29 sierpnia 1997 r. *Prawo bankowe* (t. j. Dz. U. z 2024 r. poz. 1646 ze zm.) prowadzony jest rachunek VAT oraz znajduje się w wykazie podmiotów, o którym mowa w art. 96b ustawy z dnia 11 marca 2004 r. *o podatku od towarów i usług* (t. j. Dz. U. z 2025 r. poz. 775).
9. Rozliczenie płatności wynikającej z Umowy nastąpi z uwzględnieniem mechanizmu podzielonej płatności.
10. Wykonawca złoży oświadczenie w zakresie właściwości urzędu skarbowego, w którym Wykonawca dokonuje rozliczeń.

§ 4

1. Wykonawca zapłaci Zamawiającemu kary umowne w następujących przypadkach i wysokościach:
 - 1) za zwłokę w wykonaniu któregośkolwiek z etapów realizacji przedmiotu Umowy określonych w harmonogramie, o którym mowa w rozdz. II ust. 1 OPZ – w wysokości 0,2% wynagrodzenia brutto określonego w § 3 ust. 1 za każdy rozpoczęty dzień zwłoki, licząc od dnia następującego po upływie terminu realizacji etapu, nie więcej jednak niż 15% wynagrodzenia brutto;
 - 2) za zwłokę w usunięciu stwierdzonych przez Zamawiającego wad lub braków w dokumentacji – w wysokości 0,2% wynagrodzenia brutto określonego w § 3 ust. 1 za każdy rozpoczęty dzień zwłoki, licząc od dnia wyznaczonego przez Zamawiającego na usunięcie wad lub braków, nie więcej jednak niż 10% wynagrodzenia brutto;
 - 3) za odstąpienie od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy – w wysokości 15% wynagrodzenia brutto określonego w § 3 ust. 1;
 - 4) za naruszenie obowiązku zachowania poufności w zakresie powierzonych danych i informacji Zamawiającego – w wysokości 5 000,00 zł (słownie: pięć tysięcy złotych) za każde naruszenie;
 - 5) w przypadku nieskutecznego przeniesienia autorskich praw majątkowych do opracowanej dokumentacji w zakresie określonym w § 7 – w wysokości 10% wynagrodzenia brutto określonego w § 3 ust. 1;
2. Kary umowne podlegają zsumowaniu.
3. Zapłata kar umownych nie wyłącza prawa Zamawiającego do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych, jeżeli szkoda przewyższa wysokość zastrzeżonych kar umownych.
4. Kary umowne będą potrącane przez Zamawiającego z wynagrodzenia należnego Wykonawcy, na co Wykonawca wyraża zgodę, lub dochodzone na drodze sądowej, jeśli potrącenie nie będzie możliwe.
5. Zamawiający zobowiązany jest do poinformowania Wykonawcy o naliczeniu kary umownej w terminie 14 dni od daty zaistnienia podstawy do naliczenia kary lub jej ujawnienia.

§ 5

1. Zamawiający może odstąpić od Umowy, gdy:
 - 1) Wykonawca, pomimo pisemnego wezwania ze strony Zamawiającego, określającego termin usunięcia stwierdzonych naruszeń, nie wykonuje Umowy zgodnie z opisem przedmiotu zamówienia lub w inny rażący sposób zaniedbuje lub narusza zobowiązania umowne;
 - 2) w wyniku wszczętego postępowania egzekucyjnego nastąpiło zajęcie majątku Wykonawcy lub znacznej jego części;
 - 3) Wykonawca przystąpił do likwidacji swojego przedsiębiorstwa, z wyjątkiem likwidacji przeprowadzanej w celu przekształcenia lub restrukturyzacji;
 - 4) Wykonawca powierzył wykonanie Umowy lub jej części stronie trzeciej, bez zgody Zamawiającego wyrażonej w formie pisemnej.

2. Odstąpienie od Umowy może nastąpić wyłącznie w formie pisemnej i powinno zawierać uzasadnienie.
3. Oświadczenie o odstąpieniu Strona może złożyć nie później niż w terminie 30 dni od dnia powzięcia informacji o okolicznościach, o których mowa w ust. 1.
4. Żadne z postanowień niniejszego paragrafu nie wyklucza uprawnienia Zamawiającego do odstąpienia na podstawie powszechnie obowiązujących przepisów prawa.

§ 6

1. Osobami odpowiedzialnymi ze strony Zamawiającego za:

- koordynację realizacji Umowy – jest p. Maciej Tobjasz – tel. kontaktowy 71 372 40 08; adres poczty elektronicznej (e-mail) szbi@kataster.wroc.pl,
- koordynację w zakresie ochrony danych osobowych jest p. Edyta Wasicka-Pawlus – tel. kontaktowy 71 372 40 96; adres poczty elektronicznej (e-mail) szbi@kataster.wroc.pl w porozumieniu z IOD p. Małgorzatą Czartoryską,,
- koordynację w zakresie ochrony danych z obszaru finansowo-księgowego jest p. Gabriela Sobolewska – tel. kontaktowy 71 345 99 42; adres poczty elektronicznej (e-mail) szbi@kataster.wroc.pl, w porozumieniu z IOD p. Małgorzatą Czartoryską,
- koordynację w zakresie infrastruktury IT są p. Dominik Cichoń i p. Piotr Karcz – tel. kontaktowy 71 345 99 34 lub 71 712 34 99; adres poczty elektronicznej (e-mail) szbi@kataster.wroc.pl.

2. Osobą upoważnioną do akceptacji harmonogramu, o którym mowa w rozdz. 2 ust. 1 OPZ, podpisania potwierdzenia przeprowadzenia szkolenia, o którym mowa w rozdz. III pkt 4 tiret drugie oraz podpisania protokołu odbioru, o którym mowa w § 3 ust. 4, ze strony Zamawiającego są p. Maciej Tobjasz lub p. Magdalena Zawadzka – tel. kontaktowy 71 372 40 08; adres poczty elektronicznej (e-mail) szbi@kataster.wroc.pl.

3. Osobą odpowiedzialną za nadzorowanie realizacji Umowy oraz podpisanie protokołu, o którym mowa w § 3 ust. 4 ze strony Wykonawcy jest: – tel. kontaktowy ; adres poczty elektronicznej (e-mail)

§ 7

1. Wykonawca oświadcza, że przysługiwać mu będą pełne autorskie prawa majątkowe oraz prawa do rozporządzania i korzystania z utworów stanowiących dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) opracowaną w ramach niniejszej Umowy.

2. Z chwilą odbioru przedmiotu Umowy, Wykonawca przenosi na Zamawiającego wszelkie autorskie prawa majątkowe do dokumentacji SZBI oraz prawa do wykonywania praw zależnych, bez ograniczeń czasowych i terytorialnych, na następujących polach eksploatacji:

- 1) utrwalanie i zwielokrotnianie utworu – wytwarzanie dowolną techniką egzemplarzy dokumentacji, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
- 2) wprowadzanie do obrotu, najem, użyczenie oryginału albo egzemplarzy;
- 3) wprowadzanie do pamięci komputera oraz do sieci komputerowych, w tym do sieci Internet lub intranet Zamawiającego;
- 4) publiczne udostępnianie dokumentacji w taki sposób, aby każdy mógł mieć do niej dostęp w miejscu i czasie przez siebie wybranym;
- 5) wykorzystywanie w całości lub części w działalności bieżącej Zamawiającego, w tym w związku z wykonywaniem zadań publicznych;
- 6) prawo do modyfikacji, aktualizacji, rozbudowy oraz wykorzystania fragmentów dokumentacji w innych projektach oraz do tworzenia opracowań, streszczeń i adaptacji.

3. Wynagrodzenie Wykonawcy określone w § 3 ust. 1 obejmuje pełne przeniesienie autorskich praw majątkowych oraz praw do wykonywania praw zależnych na wskazanych polach eksploatacji, a Wykonawcy nie przysługują z tego tytułu żadne dodatkowe roszczenia finansowe.
4. Wykonawca zobowiązuje się do niewykonywania autorskich praw osobistych w sposób, który mógłby ograniczać Zamawiającego w korzystaniu z dokumentacji SZBI, w szczególności zobowiązuje się do niewnoszenia sprzeciwu wobec dokonywania przez Zamawiającego zmian w dokumentacji lub jej adaptacji do potrzeb organizacyjnych i upoważnia Zamawiającego do ich wykonywania.
5. Wykonawca oświadcza, że dokumentacja SZBI nie będzie naruszać praw osób trzecich, oraz zwalnia Zamawiającego z odpowiedzialności z tytułu jakichkolwiek roszczeń osób trzecich wynikających z korzystania z dokumentacji zgodnie z przeznaczeniem, zobowiązując się do pokrycia ewentualnych kosztów związanych z roszczeniami osób trzecich.
6. W przypadku, gdy do realizacji dokumentacji SZBI Wykonawca wykorzysta utwory osób trzecich, zobowiązuje się do zapewnienia Zamawiającemu nieodpłatnej licencji niewyłącznej, nieograniczonej czasowo i terytorialnie na polach eksploatacji wskazanych w ust. 2 oraz dostarczenia Zamawiającemu stosownych oświadczeń tych osób lub kopii licencji potwierdzających prawo Wykonawcy do dysponowania utworami na warunkach umożliwiających realizację niniejszej Umowy oraz zobowiązanie do niewypowiadania licencji.
7. Na żądanie Zamawiającego Wykonawca zobowiązuje się do złożenia dodatkowych oświadczeń potwierdzających przeniesienie praw autorskich oraz praw zależnych na rzecz Zamawiającego zgodnie z treścią niniejszej Umowy.

§ 8

1. Zamawiający jako administrator danych powierza Wykonawcy przetwarzanie danych osobowych w trybie art. 28 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* w zakresie niezbędnym do wykonania Umowy.
2. Wykonawca zobowiązuje się do przetwarzania danych osobowych zgodnie z przepisami określonego w ust. 1 rozporządzenia i wyłącznie w celu realizacji Umowy.
3. Wykonawca może przetwarzać jedynie takie kategorie danych osobowych (zakres przetwarzania danych), które są niezbędne do realizacji Umowy.
4. Wykonawca nie może, bez pisemnej zgody Zamawiającego dokonywać dalszego powierzenia przetwarzania danych osobowych podmiotom trzecim (podpowierzenie). Wykonawca za działania i zaniechania podmiotów trzecich, którym powierzył dalsze przetwarzanie danych osobowych odpowiada jak za własne.
5. W kwestii ochrony danych osobowych Wykonawca zobowiązuje się do:
 - 1) zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, zmianą, utratą, uszkodzeniem lub zniszczeniem;
 - 2) zapewnienia, że osoby mające dostęp do powierzonych, w ramach niniejszej Umowy, danych osobowych są upoważnione oraz są zobowiązane do zachowania ich w tajemnicy (również po ustaniu Umowy);
 - 3) przedstawienia listy osób wykonujących czynności w zakresie przetwarzania danych udostępnionych przez Zamawiającego w celu realizacji Umowy.
6. W przypadku naruszenia przez Wykonawcę przepisów rozporządzenia, o którym mowa w ust. 1, w zakresie przetwarzania danych osobowych, w następstwie czego Zamawiający – jako administrator danych osobowych zostanie zobowiązany na podstawie prawomocnego orzeczenia sądu do wypłaty odszkodowania lub zostanie ukarany na podstawie przepisów karą grzywny, Wykonawca zobowiązuje się pokryć w całości poniesione z tego tytułu przez Zamawiającego szkody.

§ 9

1. Wszystkie informacje i dokumenty uzyskane przez Wykonawcę w związku z wykonywaniem Umowy będą traktowane jako poufne. Wykonawcę zobowiązuje się do zachowania ich w tajemnicy bez ograniczenia w czasie. Wykonawca jest zobowiązany do kontroli przestrzegania zobowiązania do zachowania w tajemnicy tych informacji przez wszystkie osoby zatrudnione przez Wykonawcę.
2. Do informacji poufnych w rozumieniu niniejszej Umowy nie zalicza się:
 - 1) informacji powszechnie dostępnych i informacji publicznych,
 - 2) informacji opracowanych przez lub będących w posiadaniu Wykonawcy przed zawarciem Umowy, o ile na mocy wcześniejszych porozumień lub umów zawartych przez Wykonawcę nie zostały one określone, jako zastrzeżone lub poufne bądź tajne lub ściśle tajne,
 - 3) informacji uzyskanych przez Wykonawcę w związku z pracami realizowanymi dla innych klientów, o ile na mocy wcześniejszych porozumień lub umów zawartych przez Wykonawcę nie zostały one określone, jako zastrzeżone lub poufne bądź tajne lub ściśle tajne.
3. Zastrzeżenie tajemnicy, o której mowa w ust. 1, nie dotyczy informacji, których ujawnienie jest wymagane przepisami obowiązującego prawa, orzeczeniami sądu lub organu władzy publicznej.

§ 10

1. W celu prawidłowego wykonania Umowy Wykonawca powierza Zamawiającemu przetwarzanie danych osobowych w zakresie imienia i nazwiska oraz danych kontaktowych osób reprezentujących Wykonawcę i realizujących zamówienie.
2. Wykonawca upoważnia Zamawiającego do przetwarzania powyżej opisanych danych osobowych w celu realizacji niniejszej Umowy oraz oświadcza, że jest upoważniony do ich przetwarzania w tym zakresie.
3. Zamawiający zobowiązuje się do przetwarzania powierzonych danych osobowych z zachowaniem przepisów rozporządzenia, o którym mowa w § 8 ust. 1 niniejszej Umowy.
4. Zamawiający zobowiązuje się do zachowania w tajemnicy wszelkich informacji poufnych, których dowiedział się w czasie realizacji zadania, jak również po wygaśnięciu Umowy z jakiegokolwiek przyczyny, bez ograniczenia w czasie.
5. Informacjami poufnymi wg ust. 4 są wszystkie informacje i dokumenty uzyskane w związku z wykonywaniem Umowy przez Zamawiającego, co do których ze względu na szczególne rozwiązania techniczne, know-how Wykonawcy lub dane finansowe Wykonawcy podjął odpowiednie środki ochronne i zastrzegł ich ochronę jako tajemnice przedsiębiorstwa wg art. 8 ust. 3 ustawy z dnia 11 września 2019 r. *Prawo zamówień publicznych* (Dz. U. z 2024 r. poz. 1320).
6. Do informacji poufnych w rozumieniu niniejszej Umowy nie zalicza się:
 - 1) informacji powszechnie dostępnych i informacji publicznych;
 - 2) informacji opracowanych przez lub będących w posiadaniu Zamawiającego przed zawarciem Umowy, o ile na mocy wcześniejszych porozumień lub umów zawartych przez Wykonawcę nie zostały one określone, jako tajemnica przedsiębiorstwa.
7. Zastrzeżenie tajemnicy, o której mowa w ust. 4 i 5 nie dotyczy informacji, których ujawnienie jest wymagane przepisami obowiązującego prawa, orzeczeniami sądu lub organu władzy publicznej.
8. Zamawiający zapewni bezpieczne przechowywanie kopii wszystkich materiałów i dokumentów objętych ochroną jako tajemnica przedsiębiorstwa Wykonawcy.

§ 11

1. Wszelkie zmiany i uzupełnienia zawartej Umowy mogą być dokonywane w formie pisemnej lub elektronicznej pod rygorem nieważności w formie aneksu, z podpisami upoważnionych przedstawicieli obu Stron.

2. Wszelkie oświadczenia Stron związane z Umową i jej wykonaniem będą kierowane w formie pisemnej za pomocą operatora pocztowego na adresy Stron Umowy lub elektronicznie na adresy poczty elektronicznej (e-mail) wskazane w § 6 niniejszej Umowy.
3. Wszelkie spory wynikające z niniejszej Umowy lub powstające w związku z Umową będą rozstrzygane przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
4. W sprawach nie uregulowanych niniejszą Umową mają zastosowanie przepisy Kodeksu cywilnego.

§ 12

1. Umowę sporządzono w formie elektronicznej w postaci pliku w formacie pdf. Oświadczenie woli każdej ze stron jest wyrażone w postaci elektronicznej i opatrzone kwalifikowanym podpisem elektronicznym.
2. Za datę umowy uznaje się dzień złożenia podpisu przez drugą ze Stron. Umowa obowiązuje z dniem jej podpisania przez obie Strony.
3. Integralną część Umowy stanowią:
 - 1) Opis Przedmiotu Zamówienia – Załącznik nr 1;
 - 2) Oferta Wykonawcy z dnia 2025 r. – Załącznik nr 2;
 - 3) Wykaz osób realizujących zadania określone w rozdz. 2 ust. 2 pkt 3 i ust. 3 pkt 3, zgodnie ze złożonym *Oświadczeniem w zakresie dysponowania zasobami osobowymi, które wykonają przedmiot zamówienia* (audytor/-rzy i specjalista ds. ochrony danych osobowych) z podaniem informacji o posiadanych certyfikatach – Załącznik nr 3.

.....
ZAMAWIAJĄCY

.....
WYKONAWCA

PZK-DA.G.222.55.2025

OŚWIADCZENIE

Jako Wykonawca: (należy podać nazwę Wykonawcy)
ubiegający się o zamówienie publiczne:

„Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Powiatowego Zakładu Katastralnego we Wrocławiu.”

oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie 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 2025 r. poz. 514), zwanej dalej „ustawą o przeciwdziałaniu”.

Na podstawie art. 7 ust. 1 ustawy o przeciwdziałaniu z postępowania wyklucza się:

- 1) wykonawcę wymienionego w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem 765/2006” i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. *w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających* (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.), zwanego dalej „rozporządzeniem 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 ustawy o przeciwdziałaniu;
- 2) wykonawcę, 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 ustawy o przeciwdziałaniu;
- 3) wykonawcę, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. *o rachunkowości* (Dz. U. z 2023 r. poz. 120) 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 ustawy o przeciwdziałaniu.

Lista osób i podmiotów (lista), wobec których są stosowane środki, o których mowa powyżej, jest prowadzona przez ministra właściwego do spraw wewnętrznych i publikowana w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw wewnętrznych.

Wykluczenie następuje na okres trwania okoliczności wskazanych powyżej, z zastrzeżeniem, że okres ten nie rozpoczyna się wcześniej niż po 30 kwietnia 2022 r.

.....
(data i podpis Wykonawcy
lub osoby uprawnionej do reprezentowania Wykonawcy)

PZK-DA.G.222.55.2025

OŚWIADCZENIE
w zakresie wskazania Naczelnika Urzędu Skarbowego właściwego dla Wykonawcy

Ja, niżej podpisany(a),

.....
(imię i nazwisko)

upoważniony(a) do jednoosobowego działania w imieniu

.....
(pełna nazwa Wykonawcy)

o nadanym numerze NIP (dalej: Wykonawca),

niniejszym oświadczam, że dla Wykonawcy właściwy jest Naczelnik

.....
(nazwa urzędu skarbowego)

.....
(adres, miejscowość)

W imieniu Wykonawcy

.....
(czytelny podpis i pieczęć)

Informujemy, że administratorem danych osobowych zbieranych przy pomocy tego oświadczenia jest Powiatowy Zakład Katastralny we Wrocławiu z siedzibą przy ul. Kościuszki 131, 50-440 Wrocław. Dane osobowe są zbierane w celu podjęcia wszelkich niezbędnych środków dla rzetelnego rozliczenia podatku. Poza podmiotami uprawnionymi na podstawie przepisów prawa zbierane dan osobowe nie będą udostępniane. Osobie, której dane dotyczą, przysługuje prawo dostępu do treści oraz poprawiania swoich danych osobowych. Podanie danych jest dobrowolne, ale niezbędne w powyżej wskazanym celu.

PZK-DA.G.222.55.2025

OŚWIADCZENIE

w zakresie dysponowania zasobami osobowymi, które wykonają przedmiot zamówienia

Jako Wykonawca: (należy podać nazwę Wykonawcy)
ubiegający się o zamówienie publiczne:

„Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Powiatowego Zakładu Katastralnego we Wrocławiu.”

oświadczam, że dysponuję zasobami osobowymi umożliwiającymi realizację zamówienia, w tym:

- 1) co najmniej jednym specjalistą posiadającym certyfikaty określone w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999), uprawniające do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077), w tym:
 - a) certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001,
 - b) certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301;
- 2) co najmniej jednym specjalistą ds. ochrony danych osobowych (inspektor ochrony danych lub osoba z doświadczeniem w realizacji projektów zgodnych z RODO), z co najmniej z dwuletnim doświadczeniem zawodowym w zakresie bezpieczeństwa informacji i ochrony danych osobowych.

.....
(data i podpis Wykonawcy
lub osoby uprawnionej do reprezentowania Wykonawcy)