

Załącznik nr 1 do SWZ– Opis przedmiotu zamówienia

Świadczenie usług „Wsparcia technicznego” dla projektu pn. „Budowa Metropolitalnego Systemu Informacji Przestrzennej (MeSIP) dla Metropolii Poznań”

Spis treści:

1	Opis przedmiotu zamówienia	3
1.1	Podstawowe informacje – zakres świadczonych usług	3
2	Wymagania szczegółowe	8
2.1	Wymagania dotyczące sposobu realizacji zamówienia	8
2.1.1	Etap 1: Przygotowanie organizacyjne, opracowanie „Planu Wsparcia”	8
2.1.2	Etap 2: Świadczenie usług doradczych, konsultacji.....	10
2.1.3	Etap 3: Przygotowanie wdrożenia systemu MeSIP, opracowanie „Metodyki wdrożenia MeSIP” ...	11
2.1.4	Etap 4: Świadczenie usług „Wsparcia technicznego” podczas wykonania Zadania II „Budowa MeSIP” 13	
2.1.5	Etap 5: Przeprowadzenie Audytu Bezpieczeństwa Systemu MeSIP.....	13
2.1.6	Etap 6: Opracowanie Raportu Końcowego i przeprowadzenie Odbioru Końcowego świadczonych usług „Wsparcia technicznego”	14
2.1.7	Etap 7: Zapewnienie świadczeń gwarancyjnych oraz z tytułu rękojmi	14
2.2	Wymagania prawne, normy techniczne, standardy i zalecenia	15
2.3	Wymagania wobec dostarczanej przez Wykonawcę dokumentacji.....	16
2.4	Wymagania techniczne dotyczące audytu MeSIP	17
2.4.1	Ocena bezpieczeństwa Infrastruktury Technicznej.....	17
2.4.2	Ocena bezpieczeństwa aplikacji WWW	19
2.4.3	Ocena zgodności rozwiązania w zakresie zgodności z obowiązującymi przepisami prawa	21
2.4.4	Ocena bezpieczeństwa przetwarzania danych osobowych	21
2.4.5	Udokumentowanie wyników audytu	22
2.5	Wymagana wobec systemu do komunikacji na odległość oraz utrzymania repozytorium dokumentów 23	
3	Dodatek nr 1 – Opis projektu	25
3.1	Założenia projektu zawarte w dokumentach inicjujących.....	25
4	Dodatek nr 2 - Studium wykonalności projektu	27
4.1	Minimalny zakres „Wsparcia technicznego”	27
5	Dodatek nr 3 - Infrastruktura Techniczna Zamawiającego, dostępne dla Wykonawcy zasoby systemowe .	28
5.1	Charakterystyka Infrastruktury Teleinformatycznej.....	28
5.1.1	Zasoby dostępne dla Wykonawcy na potrzeby prowadzenia audytu oraz niezależnych testów	28
5.1.2	Wymagania dotyczące instalacji i administrowania maszynami wirtualnymi	28
5.1.3	Zapewnienie zdalnego dostępu do Infrastruktury Technicznej	28
6	Dodatek nr 4 – Wybrane pojęcia, definicje	30

1 Opis przedmiotu zamówienia

1.1 Podstawowe informacje – zakres świadczonych usług

1. Nazwa zamówienia: **Świadczenie usług „Wsparcia technicznego” dla projektu „Budowa Metropolitalnego Systemu Informacji Przestrzennej (MeSIP) dla Metropolii Poznań”.**
2. Zamówienie stanowi część projektu pn. „Budowa Metropolitalnego Systemu Informacji Przestrzennej (MeSIP) dla Metropolii Poznań” (w skrócie Projektu) realizowanego przez Powiat Poznański w ramach Wielkopolskiego Regionalnego Programu Operacyjnego (WRPO) na lata 2014-2020: Oś Priorytetowa 2: „Społeczeństwo informacyjne” Działanie 2.1 „Rozwój elektronicznych usług publicznych”, Poddziałanie 2.1.4. dedykowane dla obszaru działań w ramach Zintegrowanych Inwestycji Terytorialnych Miejskiego Obszaru Funkcjonalnego Poznania (ZIT MOF) - Cel tematyczny 02. Zwiększanie dostępności, stopnia wykorzystania i jakości technologii informacyjnych i komunikacyjnych, Priorytet inwestycyjny 2c. Wzmocnienie zastosowań TIK dla e-administracji, e-uczenia się, e-włączenia społecznego, e-kultury i e-zdrowia. Opis projektu zawiera:
 - 2.1. Dodatek nr 1 do niniejszej specyfikacji, zawierający wprowadzenie i założenia Projektu, jakie początkowo określono w dokumentach inicjujących przedsięwzięcie,
 - 2.2. Dodatek nr 2 do niniejszej specyfikacji obejmujący w szczególności Studium Wykonalności dla przedmiotowego Projektu (zewnętrzny dokument stanowiący integralną część niniejszej dokumentacji).
3. Zamawiającym jest Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej z siedzibą w Poznaniu (PODGiK), działający w imieniu własnym oraz organu założycielskiego tj. Powiatu Poznańskiego (PP), w tym Partnerów Projektu:
 - 3.1. Stowarzyszenia Metropolia Poznań (SMP) <http://metropoliapoznan.pl/>,
 - 3.2. Miasta Poznań reprezentowanego przez Zarząd Geodezji Kartografii i Katastru Miejskiego GEOPOZ (ZGiKM GEOPOZ).
4. Przedmiot zamówienia w zakresie czynności organizacyjnych i technicznych związanych z procesem przygotowania realizacji zamówienia, a także jego wykonania, w tym przekazania i odbioru wyników prac Wykonawcy, prowadzony będzie w siedzibie Zamawiającego, adres: Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej, ul. Jackowskiego 18, 60-509 Poznań – w skrócie PODGiK.
 - 4.1. Zamawiający zaznacza, iż siedziba Zamawiającego może ulec zmianie w ciągu bieżącego roku tj. 2021na będącą aktualnie w trakcie budowy i przysposobienia: Poznań ul. Franowo 26.
5. Z uwagi na specyfikę Projektu części zadań Wykonawcy może być świadczona również w siedzibie:
 - 5.1. Lidera Projektu tj. Powiatu Poznańskiego - w Starostwie Powiatowym w Poznaniu, Poznań ul. Jackowskiego 18, w skrócie SPP,
 - 5.2. Zarządu Geodezji i Katastru Miejskiego GEOPOZ (ZGiKM GEOPOZ) w Poznaniu ul. Gronowa 20, w skrócie GEOPOZ,
 - 5.3. Stowarzyszenia Metropolia Poznań (SMP), w Biurze Stowarzyszenia Metropolia Poznań, Poznań, ul. Kościelna 37 oraz członków Stowarzyszenia Metropolia Poznań, dotyczy to okresu prac

- przygotowawczych, jakie będą w zakresie świadczeń Wykonawcy oraz czynności związanych z nadzorem technicznym nad wykonaniem testów infrastruktury MeSIP oraz przeprowadzeniem audytu systemu MeSIP i czynności odbioru. Zamawiający zakłada, iż działania Wykonawcy prowadzone w siedzibie członków SMP dotyczyć wyłącznie grupy 4-6 gmin, które aktywnie będą uczestniczyć w etapie uzgodnień projektowych i budowy prototypu systemu MeSIP, a następnie podczas pilotażu i wdrożenia docelowego rozwiązania.
6. Beneficjentem produktów niniejszego zamówienia jest Powiat Poznański. Sposób udzielenia lub przekazania Zamawiającemu praw do użytkowania opracowanych i dostarczonych przez Wykonawcę produktów stanowiących utwór zgodnie z ustawą o prawach autorskich i prawach pokrewnych określa szczegółowo projekt Umowy.
7. Zakres niniejszego zamówienia jest rozwinięciem tez oraz zakresu przedmiotowego Zadania V „Zewnętrzne wsparcie techniczne” zdefiniowanego w dokumentacji projektowej wskazanej w Dodatku nr 2 tj. w Studium Wykonalności, obejmującego czynności wsparcia technicznego i merytorycznego dla Zamawiającego w zakresie realizacji Zadania II „Budowa MeSIP”. Zamawiający zwraca uwagę, iż:
- 7.1. Zakres rzeczowy Zadania II „Budowa MeSIP”, zgodnie z dokumentacją projektową obejmuje nie tylko działania związane z przygotowaniem, dostawą, opracowaniem i wdrożeniem Systemu Informacji Przestrzennej Metropolii Poznań (w skrócie Systemu MeSIP lub MeSIP), ale także dostawę niezbędnej infrastruktury technicznej sprzętowej i oprogramowania, rozbudowę Systemu Informacji Przestrzennej Powiatu Poznańskiego (SIP PP) – i również zapewnienie koniecznej współpracy (wymiany i integracji danych) Systemu MeSIP z otoczeniem tj.:
- 7.1.1. Systemu Informacji Przestrzennej Powiatu Poznańskiego SIP PP,
- 7.1.2. Systemem Informacji Przestrzennej Miasta Poznania (SIP MP),
- 7.1.3. Systemami teleinformatycznymi gmin zrzeszonych w Stowarzyszeniu Metropolia Poznań.
- 7.2. Zgodnie z powyższym, każde sformułowanie w niniejszej specyfikacji odnoszące się do wdrożenia Systemu MeSIP musi uwzględniać zakres rzeczowy i całość uwarunkowań wykonawczych, jakie określono dla tego działania w ramach Zadania II „Budowa MeSIP” w Studium Wykonalności oraz - jakie uszczegółowiono w niniejszym dokumencie.
8. Zakres zobowiązań Wykonawcy w ramach świadczenia usług tzw. „Wsparcia technicznego” obejmuje:
- 8.1. Zarządzanie i koordynację prac zespołu Wykonawcy, w tym zapewnienie niezbędnego współdziałania z Zamawiającym, a także z każdym podmiotem:
- 8.1.1. Odpowiedzialnym za wykonanie Zadania II „Budowa MeSIP”,
- 8.1.2. Wskazany przez Zamawiającego tzw. podmiotem trzecim, który może być uprawniony do współdziałania i realizacji razem z Wykonawcą przedmiotowego zamówienia wykonując w tym zakresie czynności leżące po stronie Zamawiającego, a także prowadzącym czynności monitorowania i kontroli prac Wykonawcy.
- 8.2. Świadczenie usług doradczych, konsultacyjnych związanych z zagadnieniami technicznymi Projektu.
- 8.3. Zapewnienie wsparcia dla Zamawiającego na etapie przygotowania wdrożenia Systemu MeSIP.
- 8.4. Wsparcie realizacji Zadania II „Budowa MeSIP” poprzez zapewnienie na bieżąco wsparcia technicznego oraz merytorycznego dla Zamawiającego, w tym monitorowanie i prowadzenie oceny jakości wyników prac każdego wykonawcy przedmiotowego zadania, co w szczególności obejmuje czynności odbioru ich wyników.

- 8.5. Przeprowadzenie Audytu Bezpieczeństwa Systemu MeSIP.
- 8.6. Opracowanie Raportu Końcowego z realizacji przedmiotowego zamówienia.
- 8.7. Zapewnienie gwarancji i rękojmi obejmującej opiniowanie i konsultacje techniczne w odpowiedzi na stanowisko oraz uwagi, zastrzeżenia dot. realizacji rzeczowej Zadania II „Budowa MeSIP”, jakie zgłaszane będą przez podmioty kontrolujące Projekt, w tym w szczególności przez Instytucję Zarządzającą Wielkopolskim Regionalnym Programem Operacyjnym (IZ WRPO).
9. Poza powyższym Wykonawca jest zobowiązany do:
- 9.1. Prowadzenia z Zamawiającym wspólnej polityki informacyjnej, której podstawą dla Zamawiającego są wytyczne w zakresie promocji i polityki informacyjnej, jakie nakłada na Zamawiającego oraz Beneficjenta Instytucja Zarządzająca, co w szczególności dotyczy oznakowania pism, dokumentów zgodnie z obowiązującymi w tym zakresie wytycznymi publikowanymi na stronie <https://wrpo.wielkopolskie.pl/realizuje-projekt/poznaj-zasady-promowania-projektu/zasady-dla-umow-podpisanych-od-1-stycznia-2018-r>.
- 9.2. Raportowania, co miesiąc postępu prac oraz identyfikowanego ryzyka wykonania zamówienia w kontekście stanu realizacji Projektu (Zadania II Budowa MeSIP), co stanowić powinno wkład dla Zamawiającego do przygotowania sprawozdań z realizacji Projektu przekazywanych do IZ WRPO w okresach składania wniosków o płatność, wniosków sprawozdawczych.
10. Z uwagi na możliwe występowanie w okresie realizacji zamówienia stanu zagrożenia epidemiologicznego na terenie kraju i obowiązujące w tym okresie, ustanowione przepisami prawa określone ograniczenia, nakazy i zakazy, które mogą wpływać bezpośrednio na możliwość i sposób świadczenia usług przez Wykonawcę oraz na współdziałanie Zamawiającego oraz podmiotów zaangażowanych w realizację Projektu współpracujących z Wykonawcą:
- 10.1. Zamawiający dopuszcza możliwość świadczenia usług przez Wykonawcę drogą elektroniczną w sposób zdalny np. w formie telekonferencji, o ile zakres świadczeń, co do ich rodzaju, będzie możliwy do wykonania w ten sposób oraz, o ile wcześniej zostanie to uzgodnione i zaakceptowane przez Zamawiającego.
- 10.1.1. W tym celu Wykonawca zapewni w całym okresie realizacji zamówienia dostępność dedykowanego rozwiązania do komunikacji na odległość oraz utrzymania repozytorium dokumentów Projektu zakresie przedmiotowego zamówienia. Koszt licencji oprogramowania umożliwiającego Zamawiającemu korzystanie z tak udostępnionej infrastruktury, w tym koszt licencji zapewniającej możliwość współdziałania Zamawiającego i innych podmiotów zaangażowanych w realizację zamówienia, w tym wykonawców Zadania II „Budowa MeSIP” z Wykonawcą jest w całości i wyłącznie po stronie Wykonawcy oraz obejmuje także koszty niezbędnej infrastruktury technicznej (zasoby mocy obliczeniowej i pamięci dyskowej), którą Wykonawca musi zapewnić do niezawodnego, bezproblemowego działania zaoferowanego rozwiązania.
- 10.1.2. Zaoferowane rozwiązanie musi być dostępne w trybie 24/7/365, przy czym szczegółowe warunki związane z utrzymaniem infrastruktury np. dot. przerw technologicznych Wykonawca przedstawi i uzgodni z Zamawiającym w Planie Wsparcia. Wymagania wobec przedmiotowego oprogramowania określa Rozdział 2.5 niniejszego dokumentu.
- 10.2. Z racji, iż dla Zamawiającego zdecydowanie wyższą wartość stanowi bezpośrednie kontakt oraz współdziałanie z Wykonawcą w siedzibie Zamawiającego, Wykonawca powinien uwzględniać ryzyko i koszt wykonania zamówienia tak, jakby nie było ograniczeń wynikających ze stanu zagrożenia

epidemiologicznego. Tym samym, o ile będzie to możliwe z punktu widzenia przepisów prawa, Zamawiający może wymagać dostępności zespołu Wykonawcy w siedzibie Zamawiającego (nie częściej niż 2 razy w tygodniu, w wymiarze nie większym niż 4 godziny w danym dniu) w zakresie realizacji przedmiotu zamówienia, zgodnie z opracowanym przez Wykonawcę oraz zaakceptowanym przez Zamawiającego „Planem Wsparcia”.

10.2.1. Należy zaznaczyć, iż spotkania mają charakter tzw. „spotkań służbowych”. Zatem, o ile stan zagrożenia epidemicznego nie zostanie odwołany, spotkania te będą prowadzone z zachowaniem obowiązujących w tym zakresie przepisów prawa dot. wymogów sanitarno-epidemiologicznych, z uwzględnieniem wytycznych Ministerstwa Rozwoju, Pracy i Technologii oraz Głównego Inspektora Sanitarnego w sprawie bezpiecznego funkcjonowania poszczególnych branż gospodarki, w części dotyczącej spotkań biznesowych, szkolenia, konferencji i kongresów (*wytyczne dla branż*).

10.2.2. Skład osobowy ekspertów Wykonawcy uczestniczących w spotkaniach w siedzibie Zamawiającego będzie każdorazowo z nim uzgadniany. Przy czym w każdym spotkaniu musi uczestniczyć kierownik zespołu Wykonawcy.

10.2.1. Spotkania będą odbywały się według uzgodnionego z Wykonawcą harmonogramu. Na uzasadniony wniosek Wykonawcy, złożony przynajmniej z jednodniowym wyprzedzeniem, Zamawiający może wyrazić zgodę na zmianę harmonogramu.

11. Wykonawca jest zobowiązany zapewniać usługi „Wsparcia technicznego” w zakresie określonym w niniejszej specyfikacji do czasu zakończenia realizacji rzeczowej Zadania II „Budowa MeSIP”.

12. Uwzględniając projektowane zmiany w harmonogramie realizacji rzeczowo – finansowym Projektu, obejmujące zmianę terminu wykonania Zadania II „Budowa MeSIP” na dzień 31 maja 2023 roku oraz terminy i procedurę Odbioru Końcowego, Wykonawca jest zobowiązany świadczyć usługi „Wsparcia technicznego” do dnia zakończenia Realizacji Zadania II „Budowa MeSIP”. W przypadku zmiany terminu realizacji Projektu, w tym Zadania II „Budowa MeSIP” – zmianie ulegać będzie odpowiednio termin realizacji niniejszego zamówienia.

12.1. Zamawiający zaznacza, iż końcowy termin zakończenia realizacji Projektu może ulec zmianie wyłącznie na podstawie decyzji IZ RPO i zmianie treści umowy o dofinansowanie Projektu.

12.2. Zmiana terminu zamówienia nie stanowi podstawy do zwiększenia wynagrodzenia Wykonawcy.

13. Świadczenie usług „Wsparcia technicznego” Wykonawca powinien zapewnić w terminach i podziale na następujące etapy wykonawcze:

13.1. Etap 1: Przygotowanie organizacyjne realizacji zamówienia i opracowanie „Planu Wsparcia” – nie później niż w ciągu 14 dni od daty zawarcia umowy na realizację niniejszego zamówienia.

13.2. Etap 2: Świadczenie usług doradczych, konsultacyjnych - w sposób ciągły w całym okresie realizacji zamówienia.

13.3. Etap 3: Przygotowania wdrożenia systemu MeSIP, opracowanie „Metodyki wdrożenia MeSIP” – od daty zawarcia umowy na realizację niniejszego zamówienia nie później niż w ciągu 90 dni od daty zawarcia umowy na realizację niniejszego zamówienia.

13.4. Etap 4: Świadczenie usług „Wsparcia technicznego” podczas wykonania Zadania II „Budowa MeSIP” – do czasu odbioru ww. zadania w zakresie określonym również odpowiednio przez umowy wykonawcze podmiotów realizujących to zadanie.

- 13.5. Etap 5: Przeprowadzenie Audytu Bezpieczeństwa Systemu MeSIP – na wezwanie Zamawiającego w końcowej fazie wdrożenia MeSIP przed terminem końca Zadania II „Budowa MeSIP”, zgodnie z „Planem Wsparcia”.
- 13.6. Etap 6: Opracowanie Raportu Końcowego i przeprowadzenie Odbioru Końcowego świadczonych usług „Wsparcia technicznego” – nie później niż na 7 dni przed terminem zakończenia realizacji zamówienia.
- 13.7. Etap 7: Zapewnienie świadczeń gwarancyjnych oraz z tytułu rękojmi – od daty Odbioru Końcowego w okresie udzielonej przez Wykonawcę gwarancji i rękojmi, zgodnie z Ofertą.
14. W wykonaniu zamówienia Wykonawca uwzględnić musi wszystkie wymagania i informacje, jakie zostały zawarte w niniejszej specyfikacji, w tym także wydawane na bieżąco zalecenia Zamawiającego stanowiące wyłącznie doprecyzowanie sposobu realizacji zamówienia.

2 Wymagania szczegółowe

2.1 Wymagania dotyczące sposobu realizacji zamówienia

2.1.1 Etap 1: Przygotowanie organizacyjne, opracowanie „Planu Wsparcia”

1. W ramach czynności organizacyjnych związanych z przygotowaniem i realizacją świadczeń „Wsparcia technicznego”, Wykonawca jest zobowiązany opracować „Plan Wsparcia” stanowiący uszczegółowienie sposobu realizacji zamówienia po uwzględnieniu przez Wykonawcę wyników przeprowadzonej przez niego wstępnej analizy uwarunkowań wykonawczych i wymagań technicznych realizacji zamówienia.
2. Opracowany przez Wykonawcę „Plan Wsparcia” musi zawierać, co najmniej:
 - 2.1. Krótki opis i schemat struktury organizacyjnej powołanej do realizacji niniejszego zamówienia po stronie Wykonawcy i Zamawiającego (rola, dane kontaktowe: email, telefon) uwzględniający:
 - 2.1.1. Co najmniej kluczowy skład personelu Wykonawcy wskazany w Ofercie, w tym oddelegowaną na czas realizacji zamówienia osobę odpowiedzialną za bieżące, operacyjne zarządzanie i koordynację prac zespołu Wykonawcy i współdziałanie z Zamawiającym oraz podmiotami zewnętrznymi – dotyczy to tzw. Kierownika Wsparcia.
 - 2.1.2. Oddelegowany do współpracy z Wykonawcą ze strony Zamawiającego tzw. Zespół Projektowy obejmujący pracowników i osoby współpracujące po stronie Zamawiającego, w tym opcjonalnie wskazany przez Zamawiającego podmiot trzeci, gdzie skład osobowy zespołu jego strukturę i role Zamawiający przekaze w dniu podpisania umowy.
 - 2.1.2.1. Wykonawca musi uwzględnić konieczność aktualizacji „Planu Wsparcia” w terminie 7 dni od daty przekazania przez Zamawiającego informacji o wprowadzeniu lub zmianie oddelegowanego do współdziałania z Wykonawcą podmiotu trzeciego. O fakcie powołania takiego podmiotu Wykonawca zostanie poinformowany pisemnym oświadczeniem Zamawiającego.
 - 2.2. Harmonogram usług „Wsparcia technicznego” musi:
 - 2.2.1. Zawierać etapy, zadania, podzadania zdefiniowane w niniejszej specyfikacji oraz wskazane przez Wykonawcę, jako niezbędne dla prawidłowego wykonania zamówienia wraz z niezbędnym minimalnym ich opisem.
 - 2.2.2. Uwzględniać istotne uwarunkowania wykonawcze wynikającego z przyjętego procesu wytwórczego systemu MeSIP, jaki określono w Studium Wykonalności w zakresie realizacji Zadania II „Budowa MeSIP”.
 - 2.2.2.1. Uwaga: zmiana sposobu wytwórczego w toku realizacji zamówienia na wniosek Wykonawcy zatwierdzona przez Zamawiającego poprzez akceptację „Metodyki wdrożenia MeSIP” wymaga aktualizacji harmonogramu.
 - 2.2.3. Określić terminy dostępności informacji, danych lub zasobów, jakie są po stronie zobowiązań Zamawiającego i są niezbędne do realizacji zamówienia, dotyczy to np.: zasobów Infrastruktury Technicznej, dostępności do systemów teleinformatycznych oraz zasobów technicznych i osobowych do przeprowadzenia audytu, innych uwarunkowań.

2.2.4. Uwzględnić planowane, stałe terminy spotkań:

2.2.4.1. Koordynacyjnych Kierownika Projektu ze strony Zamawiającego z Kierownikiem Wsparcia Wykonawcy.

2.2.4.2. Technicznych Zespołu Projektowego oraz Zespołu Wykonawcy – w okresie przygotowania wdrożenia MeSIP.

2.3. Opis proponowanych przez Wykonawcę procedur zarządczych do koordynacji prac, takich jak:

2.3.1. Procedura komunikacji, obejmująca między innymi zasady dokumentowania i zatwierdzania uzgodnień, gdzie wszelkie ustalenia dotyczące sposobu realizacji zamówienia jest zobowiązany dokumentować Wykonawca w formie notatek ze spotkań i protokołów uzgodnień, których wzór musi być określony na etapie prac przygotowawczych.

2.3.2. Procedura zarządzania ryzykiem, przy czym opis użycia tej procedury musi być poprzedzony przeprowadzeniem wstępnej analizy ryzyka, celem wskazania czynników ryzyka realizacji zamówienia oraz Projektu w zakresie Zadania II „Budowa MeSIP”.

2.3.3. Procedura rozwiązywania problemów i wprowadzania zmian do realizacji zamówienia.

2.4. Harmonogram płatności uwzględniający poniższe zasady rozliczenia prac Wykonawcy:

2.4.1. Wykonanie łączne Etapu 1 oraz Etapu 3 potwierdzone bezusterkowym protokołem odbioru – nie więcej niż 20% wartości wynagrodzenia Wykonawcy,

2.4.2. Wykonanie Etapu 5 w zakresie Audytu Bezpieczeństwa Systemu MeSIP – nie więcej niż 10% wartości wynagrodzenia Wykonawcy,

2.4.3. Przeprowadzenie Odbioru Końcowego w ramach Etapu 6 – nie więcej niż 10% wartości wynagrodzenia Wykonawcy,

2.4.4. Świadczenie usług w pozostałym zakresie zobowiązań, z wyłączeniem Etapu 7 dot. świadczeń z tytułu odpowiedzialności tj. gwarancji i rękojmi – rozliczane będzie w okresach kwartalnych do 60% wartości wynagrodzenia Wykonawcy na podstawie zaakceptowanych przez Zamawiającego raportów miesięcznych opracowanych przez Wykonawcę.

2.5. Inne uwarunkowania wskazane przez Wykonawcę, jako profesjonalistę w wykonywaniu tego rodzaju zamówień, mające istotny wpływ na prawidłową i terminową realizację zamówienia oraz Projektu, w tym spełnienie wymagań Zamawiającego z punktu widzenia celu, jaki określono dla przedmiotu zamówienia, czy też zasad etyki zawodowej, jakie obowiązują personel Wykonawcy, w tym w szczególności certyfikowanych audytorów.

3. Należy podkreślić, iż dobór metod i technik koordynacji prac w zakresie realizacji zamówienia jest w gestii decyzji Wykonawcy, lecz musi być zaakceptowany przez Zamawiającego, który oczekuje w tym zakresie racjonalnego, optymalnego doboru rozwiązań zarządczych w oparciu o doświadczenie Wykonawcy z realizacji tego rodzaju podobnych zamówień bazujących.

4. Zamawiający wymaga aktualizacji „Planu Wsparcia”, w tym w szczególności Harmonogram usług „Wsparcia technicznego” po każdym zdarzeniu mającym istotny wpływ na terminy i sposób realizacji zamówienia przez Wykonawcę, między innymi dotyczy to takich okoliczności, jak:

4.1. Zidentyfikowanie nowych czynników ryzyka w zakresie realizacji niniejszego zamówienia lub realizacji Zadania II „Budowa MeSIP” – o ile mają one wpływ na przebieg zamówienia.

- 4.2. Zaakceptowanie przez Zamawiającego „Metodyki wdrożenia MeSIP”, co w szczególności obejmować może zmiany procesu wytwórczego MeSIP, a w konsekwencji tego wynikające z tego zmiany terminów oraz sposobu świadczenia usług przez Wykonawcę.
- 4.3. Zawarcie umowy z wykonawcą lub wykonawcami Zadania II „Budowa MeSIP”.
- 4.4. Wprowadzenie zmian polegających na przesunięciu określonego zakresu zobowiązań Wykonawcy pomiędzy etapami za zgodą Stron, z zachowaniem niezmienności zakresu rzeczowego całości zamówienia oraz bez uszczerbku na jakości pośrednich i końcowych wyników prac Wykonawcy, w tym końcowego wyniku realizacji Zadania II „Budowa MeSIP”, przeprowadzonych celem optymalizacji wykonania zamówienia i spełnienia celów Projektu, gdzie wszelkie tego rodzaju zmiany uważa się, za zmiany nieistotne, które nie wymagają zmiany warunków zawartej umowy z Wykonawcy, ale wymagają pisemnego uzasadnienia, które powinno zostać zawarte w zaktualizowanym „Planie Wsparcia”.
5. Aktualizację „Planu Wsparcia” Wykonawca prowadzi w sposób niezależny oraz na wezwanie Zamawiającego.
6. Zaktualizowany „Plan Wsparcia” podlega ocenie i zatwierdzeniu przez Zamawiającego.
7. Obowiązujący jest wyłącznie zatwierdzony przez Zamawiającego „Plan Wsparcia”.

2.1.2 Etap 2: Świadczenie usług doradczych, konsultacji

1. Zamawiający wymaga od Wykonawcy świadczenia usług doradczych, konsultacji w zakresie dotyczącym zagadnień, rozwiązań, produktów oraz technologii teleinformatycznych, a także metod i technik, jakie zostaną użyte do realizacji Zadania II „Budowa MeSIP”, w tym świadczenia usług przez Wykonawcę w ramach „Wsparcia Technicznego”.
 - 1.1. Powyższe dotyczy w szczególności zagadnień technicznych, uwarunkowań wykonawczych oraz ryzyka, jakie może występować w procesie budowy i wdrożenia infrastruktury technicznej, systemowej oraz aplikacyjnej MeSIP.
2. Usługi doradcze muszą być świadczone w sposób ciągły w całym okresie realizacji zamówienia.
3. W ramach ww. świadczeń Wykonawca jest zobowiązany do opiniowania ustnie i pisemnie dokumentów, specyfikacji technicznych, projektów technicznych, raportów oraz dokumentacji Projektu w zakresie wykonania Zadania II „Budowa MeSIP”, w tym opracowanej przez Wykonawcę „Metodyki wdrożenia MeSIP”, przy czym:
 - 3.1. Wydanie opinii pisemnej przez Wykonawcę musi nastąpić w ciągu 3-5 dni od daty złożenia żądania wydania takiej opinii przez Zamawiającego, gdzie dla pism i dokumentacji do 30 stron jest to okres 3 dni, a powyżej tych wielkości - maksymalnie do 5 dni.
 - 3.2. W przypadku żądania opinii w zakresie przedmiotowym świadczeń Wykonawcy przez Instytucję Zarządzającą WRPO, Wykonawca jest zobowiązany przekazać opinię w terminie umożliwiającym Zamawiającemu skuteczne, terminowe wypełnienie nałożonych na niego obowiązków informacyjnych.
 - 3.2.1. W każdym takim przypadku Zamawiający zobowiązuje się przesłać do Wykonawcy wezwanie o wydanie opinii niezwłocznie po odebraniu odpowiedniego żądania ze strony IZ WRPO.

4. Świadczenie usług doradczych obejmuje także spotkania konsultacyjne. Sposób ich przeprowadzenia Strony określać będą każdorazowo indywidualnie uwzględniając aktualne potrzeby Zamawiającego, stan realizacji Projektu oraz okoliczności poza projektowe np. uwarunkowania dot. Stanu zagrożenia epidemiologicznego.
5. Poza powyższym, w ramach świadczonych usług Wykonawca jest zobowiązany wydawać w sposób ciągły Zamawiającemu szczegółowe zalecenia na podstawie prowadzonej na bieżąco analizy stanu realizacji rzeczowej Projektu w zakresie objętym zobowiązaniami Wykonawcy dla niniejszego zamówienia.
 - 5.1. Ww. czynności Wykonawca prowadzi z tytułu odpowiedzialności za wskazany przez niego i przyjęty do realizacji przebieg wykonania Zadania II „Budowa MeSIP”, zgodny z opracowaną przez Wykonawcę „Metodyką wdrożenia MeSIP”.
 - 5.2. Wszystkie wydawane przez Wykonawcę zalecenia muszą wynikać z bieżącej oceny stanu realizacji Zadania II „Budowa MeSIP”, w tym:
 - 5.2.1. Spełniania kryteriów ilościowych i jakościowych, jakie zostały określone dla poszczególnych produktów i usług w opracowanej przez Wykonawcę „Metodyce wdrożenia MeSIP”,
 - 5.2.2. Spełnienia innych kryteriów dot. oceny zgodności realizacji procesu wytwórczego Zadania II „Budowa MeSIP” z dokumentacją projektową, co w szczególności może dotyczyć czynności zarządczych i zgodności przebiegu prac zgodnie z harmonogramem realizacji Zadania II np. w zakresie terminów punktów kontrolnych, i innych.

2.1.3 Etap 3: Przygotowanie wdrożenia systemu MeSIP, opracowanie „Metodyki wdrożenia MeSIP”

1. Przygotowanie wdrożenia systemu MeSIP poprzez opracowanie „Metodyki wdrożenia MeSIP” stanowi kluczowe zadanie Wykonawcy w zakresie usług „Wsparcia technicznego”, które powinno Zamawiającemu zapewnić osiągnięcie celów Projektu w obszarze Zadania II „Budowa MeSIP”.
2. W ramach tego etapu prac Wykonawca jest zobowiązany przeprowadzić pogłębioną analizę celów i zakresu rzeczowego Projektu na podstawie dostępnej dokumentacji Projektu oraz wywiadów z Zamawiającym, zwracając uwagę podczas analizy na kwestie dot. osiągnięcia ustalonego poziomu wartości wskaźników produktów i rezultatu projektu.
3. Wyniki analizy powinny potwierdzić i umożliwić Wykonawcy opracowanie tzw. „Założeń technicznych MeSIP” będących uszczegółowieniem koncepcji realizacji MeSIP zawartej w Studium Wykonalności, co oczywiście obejmuje nie tylko działania związane z budową Systemu MeSIP, ale również z rozbudowę Systemu Informacji Przestrzennej Powiatu Poznańskiego, współpracę z Systemem Informacji Przestrzennej Miasta Poznania oraz z współdziałanie z systemami teleinformatycznymi gmin Stowarzyszenia Metropolia Poznań w zakresie integracji i wymiany danych z MeSIP.
4. Prace Wykonawcy w ramach przedmiotowego etapu zostały podzielone na dwa podetapy:
 - 4.1. Opracowanie „Założeń technicznych MeSIP”,
 - 4.2. Opracowanie „Metodyki wdrożenia MeSIP”, do której załącznikiem i integralną częścią będą opracowanie przez Wykonawcę „Założenia techniczne MeSIP”.
5. Opracowane przez Wykonawcę „Założenia techniczne MeSIP” muszą zawierać takie zagadnienia, jak:
 - 5.1. Wnioski z pogłębionej analizy dokumentacji projektu,
 - 5.2. Koncepcja Systemu MeSIP,

- 5.3. Opis cyklu życia, w tym procesu wytwórczego Systemu MeSIP:
- 5.3.1. Wybór modelu: kaskadowy, iteracyjny prowadzony np. techniką zwinną dla fazy opracowania i uruchomienie prototypu Systemu,
 - 5.3.2. Podział zakresu funkcjonalnego oraz zakresu danych na potrzeby pilotażu obejmującego wdrożenie prototypu Systemu MeSIP,
- 5.4. Opis architektury logicznej i fizycznej Systemu MeSIP opracowany z wykorzystaniem metod i technik rekomendowanych przez metodykę TOGAF z wydzieleniem w tym opisie poszczególnych, tworzonych w ramach Projektu i Zadania II „Budowa MeSIP” systemów, podziału ich na moduły, komponenty i interfejsy komunikacyjne oraz usługi sieciowe,
- 5.5. Wymagania funkcjonalne i нефункционалне dla każdego wydzielonego elementu architektury logicznej, fizycznej MeSIP,
- 5.6. Implementacja e-usług: metody uwierzytelnienia, zdefiniowanie usług lokalnych, w tym wzoru dokumentów elektronicznych w CRWDE (Centralnym Rejestrze Wzoru Dokumentów Elektronicznych),
- 5.7. Opis infrastruktury technicznej MeSIP – koncepcja oraz wymagania wobec sieci WAN / LAN, urządzeń aktywnych, potrzeby i zasoby mocy obliczeniowej, zasoby dyskowe, bezpieczeństwo infrastruktury funkcjonowanie klastra przestrzennego, zastosowane oprogramowanie systemowe, narzędziowe, inne,
- 5.8. Harmonogram dostawy, implementacji i wdrożenia Systemu oraz infrastruktury technicznej MeSIP z wydzieleniem usług i produktów poszczególnych dostawców, włącznie z opracowaniem diagramu struktury produktów zawierającym kryteria ilościowe i jakościowe dla każdego produktu,
- 5.9. Zakres pozyskania i przetworzenia danych, dotyczy w szczególności opracowania modelu 3D dla obszaru Metropolii Poznań.
6. Punktem wyjścia do opracowania ww. założeń technicznych jest:
- 6.1. Dostępna dokumentacja projektu tj. Studium Wykonalności, w wskazany zakres świadczeń „Wsparcia technicznego” oraz udostępniona dokumentacja techniczna przez Partnera Projektu – ZGiKM GEOPOZ z wykonania Zadania V „Modernizacja Systemu Informacji Przestrzennej Miasta Poznania”,
 - 6.2. Rezultaty przeglądu dostępnych rozwiązań na rynku produktów i usług IT odpowiednio w zakresie rzeczowym Systemu MeSIP przeprowadzone przez Zamawiającego i dostępne w zasobach Wykonawcy lub wynikające z jego doświadczeń zawodowych,
 - 6.3. Projekty opcjonalnych zmian zakresu rzeczowego Projektu oraz sposobu jego wykonania w obszarze technicznym dotyczące Zadania II „Budowa MeSIP”, co w szczególności może dotyczyć zmiany terminu oraz zakresu ilościowo jakościowego dostawy infrastruktury technicznej MeSIP przez jej realizację dopiero w końcowej fazie wykonania Zadania II „Budowa MeSIP”, po opracowaniu i uruchomieniu Systemu MeSIP, dla którego wymagania zostaną zdefiniowane przez dostawcę Systemu MeSIP w zakresie wymagań wydajnościowych, pojemnościowych infrastruktury technicznej również na podstawie doświadczeń z czasowego działania systemu w oparciu o infrastrukturę chmury publicznej.
7. Poziom szczegółowości opisu, o którym mowa w pkt. 4 nie może opierać się na prezentacji wyłącznie schematów ideowych lub skrótowych zapisach też poszczególnych założeń, lecz musi zapewnić Zamawiającemu jednoznaczne niebudzące wątpliwości opisanie przedmiotu zamówienia, a Wykonawcy powinien umożliwić zaplanowanie i dobór odpowiednio metod i technik monitorowania, kontroli

i weryfikacji cech jakościowych i ilościowych produktów, dla działań, jakie są w zakresie jego zobowiązań, co w szczególności dotyczy zakresu oraz sposobu przeprowadzenia testów Systemu MeSIP, dla których to Wykonawca jest zobowiązany opracować „Metodykę testów MeSIP”.

8. Zakres opracowania „Metodyki wdrożenia MeSIP” określa poniższy konspekt dokumentacji:

- 8.1. Wstęp,
- 8.2. „Metodyka testów MeSIP” – opis standaryzacji procesu testowania systemu MeSIP od fazy planowania, przez projektowanie testów przez dostawcę systemu, po przeprowadzenie i udokumentowanie testów, które obejmować powinny testy: akceptacyjne, bezpieczeństwa, funkcjonalne, użyteczności, niefunkcjonalne, penetracyjne, regresyjne, wewnętrzne, wydajnościowe i przeciążeniowe – dokonując dla nich odpowiednio doboru rodzaju testu: black box, gray box i white box.
- 8.3. „Metodyka przeprowadzenia Audytu Systemu MeSIP” – określenie terminów oraz sposobu przeprowadzenia czynności audytu zgodnie z wymaganiami niniejszej specyfikacji,
- 8.4. Opis procedur monitorowania, kontroli i weryfikacji produktów, w tym przyjęte metody i techniki, jakie Wykonawca wdroży do realizacji swoich zobowiązań,
- 8.5. Analiza ryzyka Projektu w zakresie realizacji Zadania II „Budowa MeSIP”,
- 8.6. Słownik pojęć,
- 8.7. Załącznik: „Założenia techniczne MeSIP” (potwierdzone, zaktualizowane i uszczegółowione założenia MeSIP w zakresie wskazanym w pkt. 2).

2.1.4 Etap 4: Świadczenie usług „Wsparcia technicznego” podczas wykonania Zadania II „Budowa MeSIP”

1. Usługi „Wsparcia technicznego” w zakresie wykonania Zadania II „Budowa MeSIP” Wykonawca jest zobowiązany:
 - 1.1. Świadczyć do zakończenia realizacji umów wykonawczych w ramach Zadania II „Budowa MeSIP”.
 - 1.2. Prowadzić zgodnie z aktualnym, zatwierdzonym „Planem Wsparcia” w zakresie czynności, jakie określa „Metodyka wdrożenia MeSIP” i w terminach wynikających z harmonogramu wykonania poszczególnych umów realizacyjnych dla Zadania II „Budowa MeSIP”, w tym odpowiednio do ich stanu realizacji.
2. W okresie świadczenia usług „Wsparcia technicznego” Wykonawca jest zobowiązany razem z Zamawiającym do monitorowania i kontroli przebiegu realizacji Zadania II „Budowa MeSIP” zgodnie z przyjętym procesem wytwórczym MeSIP.

2.1.5 Etap 5: Przeprowadzenie Audytu Bezpieczeństwa Systemu MeSIP

1. Zgodnie z założeniami Projektu w końcowej fazie realizacji Zadania II „Budowa MeSIP” w zakresie wdrożenia MeSIP, odpowiednio do „Planu Wsparcia” oraz harmonogramu wykonania ww. Zadania II postrzeganego poprzez pryzmat realizowanych w tym zakresie umów, Wykonawca jest zobowiązany przeprowadzić audyt Systemu MeSIP najpóźniej przed terminem realizacji rzeczowej Zadania II „Budowa MeSIP” tak, aby zapewnić również możliwość wdrożenia działań naprawczych przez wykonawców Zadania II „Budowa MeSIP” na podstawie wyników przeprowadzonego audytu.

2. Zakres audytu W ramach tego etapu Wykonawca dokona audytu oceny bezpieczeństwa Systemu MeSIP w zakresie, jaki został ustalony dla czynności audytu z uwzględnieniem wszystkich wymagań zawartych w niniejszej specyfikacji oraz uzgodnień stron, jaki zawarto w Planie Wsparcia oraz ustaleniach bieżących.
3. Czynności w zakresie oceny podatności Infrastruktury Technicznej oraz jej bezpieczeństwa, w tym bezpieczeństwa Systemu MeSIP Wykonawca powinien przeprowadzić wykorzystując w tym celu wybrane przez siebie metody i techniki oraz specjalistyczne oprogramowanie klasy „Open Source” lub komercyjne umożliwiające ocenę podatności i możliwości przeprowadzenia testów, jak: Apache JMeter do wykonania testów funkcjonalnych, wydajnościowych, przeciążeniowych, czy też platforma Espresso lub Square KIF do automatyzacji testów.
4. Zamawiający dopuszcza prowadzenia testów systemu MeSIP w różnych porach dniach, w tym po godzinach pracy Zamawiającego. Wszelkie ustalenia dot. przeprowadzenia testów podatności oraz testów bezpieczeństwa muszą być zawierane pisemnie na bieżąco w trakcie realizacji zamówienia odpowiednio do zapisów aktualizowanego „Planu Wsparcia”.
5. Szczegółowy zakres audytu bezpieczeństwa został zamieszczony w Rozdziale 2.4.

2.1.6 Etap 6: Opracowanie Raportu Końcowego i przeprowadzenie Odbioru Końcowego świadczonych usług „Wsparcia technicznego”

1. Nie później niż na 7 dni przed terminem zakończenia realizacji zamówienia Wykonawca opracuje Raport Końcowy z realizacji zamówienia podsumowujący wykonanie usługi „Wsparcia technicznego”.
2. Zamawiający dokona Odbioru Końcowego po weryfikacji Raportu Końcowego oraz po potwierdzeniu wypełnienia przez Wykonawcę wszystkich zobowiązań, jakie były przedmiotem realizacji niniejszego zamówienia.
 - 2.1. Podczas czynności odbioru Wykonawca jest zobowiązany do ścisłego współdziałania z Zamawiającym, w tym składania niezbędnych wyjaśnień oraz skutecznego i niezwłocznego wypełnienia potencjalnie niezrealizowanych, zaległych zobowiązań.
3. W trakcie Odbioru Końcowego zamówienia, Wykonawca złoży oświadczenie, potwierdzające kompletność wykonania zamówienia z punktu widzenia zakresu rzeczowego, przedmiotu oraz, iż zostały prawidłowo wykonane zgodnie z wymaganiami określonymi w OPZ, a także zgodnie z wytycznymi, jakie zostały przekazane Wykonawcy przez Zamawiającego w trakcie realizacji zamówienia.
4. Wszelkie niezbędne korekty, uzupełnienia, jakie mogą wynikać z wezwania Wykonawcy do usunięcia zidentyfikowanych podczas Odbioru Końcowego uchybień, Wykonawca jest zobowiązany skorygować w terminie wskazanym przez Zamawiającego. Powyższe odnosi się do wszystkich świadczeń Wykonawcy, w tym może dotyczyć również odebranych raportów miesięcznych stanowiących podstawę do rozliczenia kwartalnego wynagrodzenia Wykonawcy, o ile wymagać będą one uzupełniania lub korekty na podstawie informacji oraz wiedzy, jaką Zamawiający posiadał dopiero podczas czynności Odbioru Końcowego.

2.1.7 Etap 7: Zapewnienie świadczeń gwarancyjnych oraz z tytułu rękojmi

1. Od daty Odbioru Końcowego w okresie udzielonej przez Wykonawcę gwarancji i rękojmi, zgodnie z zapisami zawartej umowy, Wykonawca jest zobowiązany do świadczenia usług gwarancyjnych oraz z tytułu rękojmi.
2. Zakres tych świadczeń obejmuje udzielenie opinii ustnie i pisemnie na wniosek Zamawiającego w przypadku konieczności wydania opinii dot. realizacji świadczeń przez Wykonawcę lub realizacji i wykonania Zadania II „Budowa MeSIP”, o jaką wystąpią organy kontrolne, w tym w szczególności Instytucja Zarządzająca WRPO.

3. W odpowiedzi na wezwanie Zamawiającego i żądanie wydania opinii Wykonawca jest zobowiązany przygotować i przekazać wypracowane przez siebie stanowisko w terminie umożliwiającym Zamawiającemu skuteczne, terminowe wypełnienie nałożonych na niego obowiązków informacyjnych w wezwaniu organu kontrolującego.

3.1. W każdym przypadku Zamawiający zobowiązuje się przelać do Wykonawcy wezwanie o wydanie opinii niezwłocznie po odebraniu odpowiedniego żądania ze strony organu kontrolującego.

2.2 Wymagania prawne, normy techniczne, standardy i zalecenia

1. Zamówienie musi być realizowane z uwzględnieniem obowiązujących przepisów prawa w zakresie projektowania, wdrażania i wykorzystania systemów teleinformatycznych przez podmioty realizujące zadania publiczne oraz przepisów prawa w obszarze dziedzinowym projektowanych rozwiązań (między innymi wskazanych w Dodatku nr 2 – Studium Wykonalności), w tym dotyczącym ochrony danych osobowych, a w szczególności takich jak:

1.1. Ustawy:

- Ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2020 r. poz. 346 z późn. zm.),
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781, t.j.),
- Ustawa z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz.U. z 2018 r., poz. 1472 t.j.),
- Ustawa z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2019 r. poz. 848),
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U.2020 1369)

1.2. Rozporządzenia:

- Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 10 września 2010 roku w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz. U. z 2010 r. Nr 177 poz. 1195),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 20 października 2010 r. w sprawie ewidencji zbiorów i usług danych przestrzennych objętych infrastrukturą Informacji przestrzennej (Dz. U. z 2010 r. Nr 201, poz. 1333 z późn. zm.),

1.3. Przepisy unijne:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwane dalej RODO (Dz.U.UE.L. z 2016r nr 119 poz.1 z późn. zm),
- Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z 14 marca 2007 r. ustanawiająca infrastrukturę Informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE) (Dz.U.UE.L. z 2007r. nr 108 poz. 1 z późn. zm.),
- Rozporządzenie Komisji (WE) NR 976/2009 z dnia 19 października 2009 r. w sprawie wykonania dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady w zakresie usług sieciowych i Rozporządzenie Komisji (WE) NR 1205/2008 z dnia 3 grudnia 2008 r. w sprawie wykonania dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady w zakresie metadanych (Dz.U.UE.L. z 2009r nr 274 poz.9 z późn. zm),

- Rozporządzenie Komisji (UE) nr 1089/2010 z dnia 23 listopada 2010 r. w sprawie wykonania dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady w zakresie interoperacyjności zbiorów i usług danych przestrzennych (tekst skonsolidowany) (Dz.U.UE.L. z 2010r nr 323 poz.11 z późn. zm).
- 2. W realizacji zamówienia Zamawiający zaleca zastosowanie norm i standardów technicznych wg. Polskich Normy (PN) wprowadzających z Sektora Technika informatyczna – Technika bezpieczeństwa takich, jak:
 - 2.1.1. PN-EN ISO/IEC 27000:2017-06 Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia,
 - 2.1.2. PN-EN ISO/IEC 27001:2017-06 Systemy zarządzania bezpieczeństwem informacji – Wymagania,
 - 2.1.3. PN-ISO/IEC 27005:2010 Zarządzanie ryzykiem w bezpieczeństwie informacji,
 - 2.1.4. PN-ISO/IEC 29151:2019-01 Praktyczne zasady ochrony informacji o identyfikowalnych osobach,
 - 2.1.5. PN-ISO/IEC 29134:2018-11 Wytyczne dotyczące oceny skutków dla prywatności.
- 3. W uzupełnieniu powyżej wskazanych norm Wykonawca może stosować Polską Normę PN-I-13335-1:1999 Wytyczne do zarządzania bezpieczeństwem systemów informatycznych -- Pojęcia i modele bezpieczeństwa systemów informatycznych – w zakresie niesprzecznym z obowiązującym przedmiotowo normami wprowadzającymi.
- 4. Do norm wskazanych w pkt. 2, 3 Zamawiający dopuszcza zastosowanie norm równoważnych.
- 5. Ponadto, w sposobie realizacji zamówienia Wykonawca powinien uwzględnić:
 - 5.1. Standardy prowadzenia audytu, odpowiednio do wynikające z certyfikacji, jakie posiada jego personel, a jakie zostały wydane przez np. Stowarzyszenie Audytorów Systemów Informatycznych ISACA, Instytut Audytorów Wewnętrznych IIA.
 - 5.1.1. Zakres zastosowania standardów dot. prowadzenia audytów, jak również norm i standardów technicznych powinien zostać określony w Planie Audytu.
 - 5.2. Zalecenia dot. sposobu i technik przeprowadzenia testów bezpieczeństwa dla aplikacji WWW, jakie są publikowane przez fundację non-profit OWASP (ang. Open Web Application Security Project), w szczególności dotyczy tzw. OWASP – Top Ten.
- 6. Czynności związane z przeprowadzeniem audytu systemu MeSIP muszą być prowadzone pod nadzorem merytorycznym Głównego Audytora, posiadającego kompetencje uprawniające do audytu i kontroli systemów teleinformatycznych, o których mowa w załączniku do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych.

2.3 Wymagania wobec dostarczanej przez Wykonawcę dokumentacji

1. W każdym przypadku, kiedy następować będzie przekazanie dokumentacji opracowanej przez Wykonawcę, na żądanie Zamawiającego musi być ona przekazana w formie papierowej, w liczbie jednego egzemplarza z każdego rodzaju oraz w formie elektronicznej przesłana drogą elektroniczną na adres e-mail Zamawiającego (lub na adres podany w „Planie Wsparcia”) lub przekazana na nośniku CD-ROM, i tak dla:
 - 1.1. dokumentacji w formie opracowania w formacie edytowalnym: ODF lub DOC / DOCX oraz zabezpieczonym przed edycją formacie PDF dla programu Acrobat Reader,

- 1.2. wyników prac w formie arkusza kalkulacyjnego w formacie MS Excel: ODS, XLSX,
- 1.3. dokumentacji w formie modelu architektury korporacyjnej wg metodyki TOGAF – odpowiednio w formacie natywnym użytego do tego celu oprogramowania.

2.4 Wymagania techniczne dotyczące audytu MeSIP

2.4.1 Ocena bezpieczeństwa Infrastruktury Technicznej

1. Ocena bezpieczeństwa Infrastruktury Technicznej obejmuje ocenę środowiska technicznego: urządzeń dostępowych, sieciowych, środowiska systemowego, narzędziowego (uruchomieniowego MeSIP), w zakresie, co najmniej wskazanych poniżej obszarów.
2. Analiza topologii sieci komputerowej (LAN, WAN) – obejmuje również układ klastra przestrzennego:
 - 2.1. Celem tego zadania jest analiza logicznej i fizycznej topologii sieci oraz reguł kierowania ruchem sieciowym. Do analizy należy brać urządzenia aktywne i ich zadania w zakresie kierowania i obsługi ruchu sieciowego, a także wszystkie urządzenia budujące topologię systemu – routery, systemy firewall, przełączniki sieciowe, elementy systemu IDS / IPS. W raporcie z tego zakresu prac Wykonawca przedstawi:
 - 2.1.1. Ocena konstrukcji topologii sieci pod kątem ogólnych zasad budowy tego typu systemów,
 - 2.1.2. Ocenę topologii pod kątem zasięgu ruchu sieciowego w poszczególnych segmentach systemu,
 - 2.1.3. Ocenę topologii sieci pod kątem niezawodności i redundancji poszczególnych elementów systemu,
 - 2.1.4. Ocenę topologii pod kątem możliwości przeprowadzenia ataku zdalnego,
 - 2.1.5. Potencjalne cele ataku i źródła ataków,
 - 2.1.6. Wskazówki dotyczące zwiększenia poziomu bezpieczeństwa systemu poprzez modyfikację topologii sieci.
3. Analiza usług systemowych:
 - 3.1. Wykonawca przeprowadzi analizę usług systemowych udostępnianych zdalnie jak również lokalnie w obszarze poddanym badaniu. W raporcie z tego zakresu prac Wykonawca przedstawi:
 - 3.1.1. Zakres uruchomionych usług – na potrzeby systemu,
 - 3.1.2. Usługi wymagane dla zapewnienia identyfikowanej funkcjonalności,
 - 3.1.3. Analizę ruchu sieciowego związanego z usługami oraz administracją, przepływającego pomiędzy poszczególnymi strefami – segmentami systemu / sieci,
 - 3.1.4. Usługi uruchomione nadmiarowo,
 - 3.1.5. Usługi niestwarzające realnego niebezpieczeństwa ataku,
 - 3.1.6. Usługi stwarzające realne niebezpieczeństwo ataku.
4. Analiza poprawności konfiguracji urządzeń dostępowych, sieciowych:
 - 4.1. W ramach tego zadania Wykonawca przeprowadzi przegląd konfiguracji sprzętowej i programowej wszystkich urządzeń aktywnych wchodzących w skład Infrastruktury Technicznej obsługującej ruch

sieciowy audytowanego systemu. Analiza prowadzona będzie pod kątem istnienia komponentów wymagających uaktualnienia oraz instalacji poprawek systemowych. Przeprowadzona zostanie również analiza poprawności:

- 4.1.1. Konfiguracji routerów i serwerów dostępowych,
- 4.1.2. Konfiguracji i przepływów systemów firewall,
- 4.1.3. Konfiguracji elementów systemu IDS / IPS, jeżeli takowe istnieją,
- 4.1.4. Konfiguracji przełączników sieciowych,
- 4.1.5. Zastosowanych wersji oprogramowania i systemów operacyjnych ww. elementów systemu.
- 4.1.6. Konsoli zarządzających poszczególnymi elementami systemu,
- 4.1.7. Systemów operacyjnych poszczególnych urządzeń aktywnych systemu.

5. Analiza procedur zarządzania, administrowania:

- 5.1. Wykonawca dokona oceny przygotowania, kompletności oraz poprawności merytoryczne procedur administracji i zarządzania infrastrukturą techniczną w obszarze audytu w zakresie udostępnionych przez Zamawiającego materiałów, dokumentów oraz informacji pozyskanych na podstawie przeprowadzonych wywiadów.

6. Analiza i testy bezpieczeństwa.

- 6.1. Testy bezpieczeństwa obejmą krytyczne elementy Infrastruktury Technicznej i funkcje systemowe w celu zidentyfikowania zagrożeń lub potwierdzenia wskazanych przez wyniki analizy parametrów technicznych i konfiguracji urządzeń. Zakres podejmowanych czynności Wykonawcy obejmie takie podzadania jak:

- 6.1.1. Analiza penetracyjna: Celem tego zadania jest wykonanie badania podatności konfiguracji infrastruktury „z zewnątrz”. Analiza dotyczyć będzie zarówno usług, które są zdefiniowane oraz udostępniane przez system dla sieci zewnętrznych i usługobiorców (np. dla sieci Internet), jak również może wykazywać podatność na próby penetracji i sprawdzania wszystkich dostępnych usług. Na podstawie raportu wygenerowanego przez wybrane przez Wykonawcę narzędzia np. skanery sieciowe oraz wnioski z analizy usług, analizy topologii sieci zostanie przygotowany raport zawierający:

- 6.1.1.1. Nieprawidłowości w konfiguracji bezpieczeństwa systemu,

- 6.1.1.2. Wskazówki dotyczące sposobu usunięcia nieprawidłowości.

- 6.1.2. Włamanie kontrolowane: W tym zadaniu zostanie przeprowadzona próba włamania przy użyciu metod nieinwazyjnych. Tego rodzaju atak jest prawie 100% odzwierciedleniem rzeczywistej próby włamania. Działania te zostaną udokumentowane w końcowym raporcie. Taka metoda pozwala na wykrycie potencjalnych luk w systemie zabezpieczeń infrastruktury IT audytowanego systemu.

- 6.1.3. Analiza bezpieczeństwa serwerów (klastra): Zadanie obejmuje czynności badania i oceny bezpieczeństwa serwerów, które można podzielić na trzy grupy:

- 6.1.3.1. Prace analityczne: badanie poprawności konfiguracji systemów operacyjnych oraz ich administracji pod względem bezpieczeństwa i analiza wyników.

- 6.1.3.2. Ewidencja znalezionych luk bezpieczeństwa wraz z opisami metod ich eliminacji (zbadane luki w oprogramowaniu za pomocą testerów podatności ang. vulnerability scanner).
- 6.1.3.3. Prace naprawcze (hardening): wytyczne w zakresie eliminacji luk bezpieczeństwa zgodnie z wskazaniami zawartymi w raportach „po testowych”.
- 6.1.4. Analiza przepływności: Celem zadania jest ocena przepływności ruchu pomiędzy strefami bezpieczeństwa z uwzględnieniem podziału na strefy serwerów bazy danych, serwerów aplikacji DMZ (i inne), z odniesieniem do wyników weryfikacji poziomu logowania na urządzeniach brzegowych (firewall) dla sesji nawiązywanych pomiędzy krytycznymi strefami bezpieczeństwa.
- 6.1.5. Analiza systemu monitorowania: Zadanie podlega na ocenie działającego systemu monitoringu systemów wystawionych na ataki z zewnątrz. Testy będą przeprowadzone w obszarach krytycznych na styku połączeń Internet – strefa DMZ, strefa DMZ- serwery aplikacyjne, serwery aplikacyjne – serwery baz danych.
- 6.2. Zakres prac audytorskich może zostać rozszerzony o obszary i zagadnienia, jakie Wykonawca wskaże, jako kluczowe do oceny stanu Infrastruktury Technicznej podczas opracowania Planu Wsparcia. Zakres tych prac i ich koszt zostanie wyceniony, a następnie rozliczony w godzinach konsultacji technicznych, jakie zostały przewidziane w ramach niniejszego zamówienia.
7. Ocena bezpieczeństwa maszyn wirtualnych (VM) i zdefiniowanych w nich środowisk uruchomieniowych musi być przeprowadzona odrębnie dla każdej wydzielonej części systemu MeSIP.

2.4.2 Ocena bezpieczeństwa aplikacji WWW

1. Testy bezpieczeństwa obejmują poniższe testy oceny podatności oraz wycinkową ocenę wydajności systemu MeSIP, w zakresie aplikacji WWW.
2. Testy bezpieczeństwa aplikacji:
 - 2.1. W ramach tego zadania Wykonawca przeprowadzi testy bezpieczeństwa (black box, grey box), wśród których powinny znaleźć się zawsze testy z aktualnej listy dziesięciu najpopularniejszych ataków sieciowych tzw. OWASP TOP 10 (<https://owasp.org/www-project-top-ten/>). Minimalny, wymagany zakres testów zawiera:
 - 2.1.1. Test penetracyjny styku z Internetem (przy konfiguracji produkcyjnej) – w tym skuteczności urządzeń IDS/IPS.
 - 2.1.2. Manipulacje parametrami.
 - 2.1.3. Techniki podsłuchu i manipulowania transmisją (w tym Man in The Middle).
 - 2.1.4. Wywołanie strony serwisu spoza ścieżki przewidzianej przez projektantów aplikacji (Forcefull browsing).
 - 2.1.5. Atak Path Traversal.
 - 2.1.6. Technika Google Hacking (dotyczy aplikacji opublikowanych w sieci Internet).
 - 2.1.7. Filtrowanie danych wejściowych.
 - 2.1.8. Omijanie filtrowania danych wejściowych i wyjściowych.
 - 2.1.9. Ataki na sesję aplikacji webowej (session fixation i session adoption).

2.1.10. Ataki typu Injection (np. SQL/XML/XPath/HTML/LDAP oraz innych zgodnie z technologią aplikacji) i Blind SQL Injection.

2.1.11. Ataki XSS - Cross Site Scripting (persistent, reflected, itp.), czyli osadzenie obcego skryptu.

2.1.12. Niepoprawna obsługa uwierzytelniania i sesji.

2.1.13. Niezabezpieczone bezpośrednie odwołanie do obiektu (Insecure Direct Object References).

2.1.14. Fałszowanie żądań (CSRF - Cross Site Request Forgery).

2.1.15. Niepoprawne ustawienia (Security Misconfiguration).

2.1.16. Brak zabezpieczeń dostępu przez URL (Failure to Restrict URL Access).

2.1.17. Brak walidacji przekierowań (Unvalidated Redirects and Forwards).

2.1.18. Błędy szyfrowania danych (Insecure Cryptographic Storage).

2.1.19. Niedostateczne zabezpieczenia wymiany danych (Insufficient Transport Layer Protection).

2.1.20. Atak typu brute force (sprawdzenie czy konto lub adres IP zostanie zablokowane).

2.1.21. Testy dotyczące ujawniania informacji o środowisku hostującym.

2.1.22. Testy typu DoS (np. flooding).

2.1.23. Ataki typu spoofing.

2.1.24. Ocena kompletności zbieranych informacji w logach.

2.1.25. Ataki w celu rozpoznania aplikacji i platformy.

2.1.26. Próba podniesienia uprawnień.

2.1.27. Przekazanie wrażliwych danych w adresie URL lub podmiana wartości parametrów UR.

2.1.28. Modyfikacje treści strony w aplikacji internetowej.

2.1.29. Wymuszenie kodów błędów HTTP500, czy też HTTP400, HTTP300, aby uzyskać informacje o strukturze katalogów serwera WWW.

2.1.30. Zdradzenie nadmiarowych danych np. nazwy i wersji serwera aplikacji.

2.1.31. Nawiązywanie równoległych połączeń przy tych samych danych użytkownika (login / hasło), czy też dopuszczenie do próby obejścia zastosowanych zabezpieczeń np. blokada konta po nieudanych próbach logowania itp.

2.2. Testy wydajności, testy obciążeniowe:

2.2.1. W ramach tego zadania wykonawca dokona oceny stabilności działania systemu przy określonym, przyjętym i podanym przez Zamawiającego poziomie obciążenia. Wykonawca dokona oceny przeciążenia systemu (pośrednio ocena wydajności systemu) wykorzystując do tego specjalistyczne oprogramowanie umożliwiające automatyzację testów.

3. Testy bezpieczeństwa muszą być przeprowadzone zgodnie z ustaleniami zawartymi w „Planie Wsparcia” odpowiednio w środowisku testowym lub produkcyjnym, przez prowadzenie testów z wewnątrz infrastruktury technicznej Zamawiającego oraz odrębnie w środowisku zewnętrznym.

2.4.3 Ocena zgodności rozwiązania w zakresie zgodności z obowiązującymi przepisami prawa

1. W ramach czynności związanych z oceną zgodności systemu MeSIP z obowiązującymi przepisami prawa Wykonawca dokona analizy oraz oceny zgodności przyjętych rozwiązań organizacyjnych i technicznych systemu MeSIP w zakresie, w jakim nakłada obowiązki na Zamawiającego ustawodawca przepisami:
 - 1.1. Ustawy z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2019 r. poz. 848) – weryfikacja spełnienia wymagań WCAG 2.0 / 2.1.
 - 1.2. Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U.2020 poz. 1369).
 - 1.3. Rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz.2247).
 - 1.3.1. W czynnościach prowadzonej przez Wykonawcę analizy należy posługiwać się wytycznymi opublikowanymi przez Ministerstwo Cyfryzacji w zakresie kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych – link do wytycznych: <https://www.gov.pl/web/cyfryzacja/wytyczne-dla-kontroli-dzialania-systemow-teleinformatycznych-uzywanych-do-realizacji-zadan-publicznych-zatwierdzone-przez-ministra-cyfryzacji>
2. Wyniki analizy i oceny zgodności muszą przybrać formę szczegółowych rekomendacji, w których zawarte zostaną uwagi będące opisem zidentyfikowanych odstępstw, braków - oraz szczegółowe zalecenia dot. wdrożenia procedur naprawczych.

2.4.4 Ocena bezpieczeństwa przetwarzania danych osobowych

1. W ramach tego zadania na podstawie dokumentacji systemu MeSIP i przeprowadzonej przez Wykonawcę analizy technicznej wdrożonych rozwiązań technicznych i organizacyjnych, popartych oceną udostępnionej przez Zamawiającego analizy ryzyka będącą składową wstępnie opracowywanej przez Zamawiającego oceny skutków ochrony danych osobowych w zakresie planowanych operacji przetwarzania danych nowego systemu teleinformatycznego MeSIP (Systemu MeSIP, Systemu SIP PP, usług integracji z systemami teleinformatycznymi członków Stowarzyszenia Metropolia Poznań), Wykonawca bazując na własnym doświadczeniu oraz na podstawie wytycznych „Grupy Roboczej Artykuł 29”, dokona oceny skutków ochrony danych osobowych w procesach przetwarzania danych przedmiotowego Systemu MeSIP.
2. W tym celu Wykonawca współdziałając razem z Zamawiającym, w szczególności z Inspektorem Ochrony Danych Osobowych (IOD):
 - 2.1. Dokona oceny przyjętych rozwiązań technicznych oraz wdrożonych zabezpieczeń procesu przetwarzania danych osobowych,
 - 2.2. Opcjonalnie – zależnie od potrzeb, przeprowadzi dodatkowe testy w celu wykazania podatności w obszarze przetwarzania danych osobowych,
 - 2.3. Opracuje ocenę skutków przetwarzania danych osobowych (DPIA) zgodnie z art. 35 RODO uwzględniając w tym:
 - 2.3.1. Pozyskaną wiedzę nt. rozwiązań technicznych,
 - 2.3.2. Wyniki testów bezpieczeństwa Systemu, w tym wyniki testów podatności, o których mowa na wstępie,

2.3.3. Zalecenia, jakie wynikają z normy PN-ISO/IEC 29134: 2018-11 Wytyczne dotyczące oceny skutków dla prywatności lub innej normy równoważnej.

3. Na podstawie uzyskanych wyników Wykonawca wyda rekomendacje i opracuje projekt zmian do Polityki Bezpieczeństwa Informacji Zamawiającego.

2.4.5 Udokumentowanie wyników audytu

1. Wyniki przeprowadzonego audytu MeSIP w zakresie określonym w niniejszej specyfikacji muszą zostać szczegółowo udokumentowane w formie Raportu z Audytu, który powinien zawierać:
 - 1.1. Opis skrócony dla Kierownictwa.
 - 1.2. Podsumowanie założeń organizacyjnych i technicznych dot. zakresu i sposobu przeprowadzenia audytu.
 - 1.3. Opis przyjętej metodyki oraz technik przeprowadzenia audytu.
 - 1.4. Klauzule poufności zgodnie z zasadami etyki zawodowej certyfikowanych audytorów.
 - 1.5. Udokumentowanie wszystkich czynności związanych z sprawdzeniem i oceną stanu infrastruktury technicznej tj. sprzętu komputerowego i oprogramowania, w tym, co najmniej:
 - 1.5.1. Opis przeprowadzonych analiz i testów, wraz z opisem zastosowanych metod i narzędzi oraz uzyskanych wyników pośrednich i końcowych, co w szczególności dotyczy:
 - 1.5.1.1. Wyników z testów bezpieczeństwa, w tym głównie zdarzeń / incydentów będących podstawą do wskazania rekomendowanych zmian w konfiguracji środowiska systemowego / aplikacyjnego, a w przypadku identyfikacji niezgodności lub niezastosowania się do dobrych praktyk, czy też wymagań KRI – wdrożenia działań korygujących.
 - 1.5.1.2. Wyniki oceny zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa.
 - 1.5.2. Rekomendowane opisy konfiguracji Infrastruktury Technicznej.
 - 1.5.3. Inne zalecenia, w tym w szczególności zalecenie dotyczące spełnienia wymagań KRI.
 - 1.6. Wyniki analizy i ocena zgodności przetwarzania danych odpowiednio do obowiązujących przepisów prawa, w szczególności w zakresie wynikającym z obowiązku stosowania RODO.
 - 1.7. Określenie poziomu zgodności w każdym z obszarów przeprowadzonego audytu.
 - 1.8. Wnioski końcowe:
 - 1.8.1. Sumaryczna ocena zgodności.
 - 1.8.2. Rekomendacje dot. działań naprawczych i korygujących.
 - 1.8.3. Projekt zmian do Polityki Bezpieczeństwa Informacji Zamawiającego.
 - 1.9. Załączniki:
 - 1.9.1. Dokumentacja źródłowa z audytu.
 - 1.9.2. Oświadczenia imienne certyfikowanych audytorów.

1.9.3. Oświadczenie Wykonawcy.

2. W Raporcie muszą znaleźć się wszystkie informacje, wyniki i wnioski, o których mowa w opisie wymagań dla prowadzonych przez Wykonawcę analiz i testów Infrastruktury Technicznej.
3. Zamawiający dopuszcza inny układ i strukturę Raportu z Audytu bez zmiany zakresu rzeczowego raportu. Proponowany przez Wykonawcę konspekt raportu np. oparty o wybraną przez wykonawcę metodykę przeprowadzenia audytu, musi zostać zaakceptowany przez Zamawiającego na etapie opracowania „Planu Wsparcia”.
4. Raport z Audytu ma status informacji poufnej i zawierać musi następujące oświadczenia:
 - 4.1. Oświadczenie imienne certyfikowanych audytorów o zachowaniu poufności, w tym wszelkich udostępnionych i przekazanych Wykonawcy przez Zamawiającego informacji i materiałów, w tym w szczególności zdobytych w trakcie prac informacyjnych.
 - 4.2. Oświadczenie Wykonawcy o zachowaniu poufności oraz o usunięciu wszystkich kopii danych, dokumentów oraz wszelkich materiałów, które znalazły się w jego władaniu w okresie realizacji zamówienia. Do oświadczenia należy dołączyć protokół zniszczenia kopii materiałów i dokumentów.

2.5 Wymagana wobec systemu do komunikacji na odległość oraz utrzymania repozytorium dokumentów

1. Oferowane przez Wykonawcę dedykowane oprogramowanie musi:
 - 1.1. Zapewnić działanie poprzez aplikację webową dostępną z poziomu przeglądarki internetowej,
 - 1.2. Umożliwić jednoczesną pracę wielu użytkowników bez nakładania ograniczeń na ich liczbę, przy czym ewentualne ograniczenia mogą dotyczyć wyłącznie ograniczeń infrastruktury w zakresie jej wydajności,
 - 1.3. Zapewnić mechanizmy zarządzania użytkownikami, w tym nadawania im uprawnień,
 - 1.4. Wspomagać czynności zarządzania projektem – minimum w zakresie procedur komunikacji i powiadamiania,
 - 1.5. Zapewniać mechanizmy autoryzacji dostępu, w tym zastosowanie bezpiecznych połączeń np. z zastosowaniem protokołu TLS,
 - 1.6. Posiadać co najmniej następujące moduły/narzędzia: narzędzie do wideokonferencji, serwer/repozytorium plików, narzędzie do pracy współdzielonej nad dokumentami.
2. Narzędzie do wideokonferencji powinno umożliwiać:
 - 2.1. Tworzenie wideokonferencji i zapraszanie użytkowników zarejestrowanych i/lub niezarejestrowanych (tzw. gości, zapraszanych np. poprzez link do danej wideokonferencji) w systemie,
 - 2.2. Udostępnianie treści/widoku ekranu użytkownika dla uczestników zdalnego spotkania,
 - 2.3. Prowadzenie rozmowy również w formie czatu dla każdego pokoju (zdefiniowanej grupy użytkowników),
 - 2.4. Identyfikację statusu dostępności użytkownika (przynajmniej w zakresie: aktywny, nieaktywny, zajęty),

- 2.5. Mechanizm powiadomień, w tym wywołań użytkowników w trybie czatu.
3. Serwer/repozytorium plików powinien umożliwiać:
 - 3.1. Tworzenie katalogów projektowych,
 - 3.2. Udostępnianie katalogów w ramach zdefiniowanych grup użytkowników lub bezpośrednio użytkownikom w dwóch trybach: tylko podglądu lub pełnego dostępu i edycji dokumentów,
4. Narzędzie do pracy współdzielonej nad dokumentami musi zapewnić:
 - 4.1. Pracę na dokumentach tekstowych, arkuszach kalkulacyjnych i prezentacjach,
 - 4.2. Edycję dokumentu przez wielu użytkowników jednocześnie,
 - 4.3. Włączenie trybu śledzenia zmian oraz wykorzystania komentarzy w ramach pracy wspólnej na dokumentach tekstowych,
 - 4.4. Identyfikację wersji dokumentów (zapis automatyczny),
 - 4.5. Obsługę formatów plików: docx, xlsx, pptx.

3 Dodatek nr 1 – Opis projektu

3.1 Założenia projektu zawarte w dokumentach inicjujących

Stowarzyszenie Metropolia Poznań (SMP), inaczej Metropolia Poznań – to stowarzyszenie gmin i powiatów Aglomeracji Poznańskiej, które powstało w 2011 roku. Stowarzyszenie obejmuje Miasto Poznań, Powiat Poznański, 17 gmin powiatu poznańskiego oraz 4 gminy sąsiednie. Zasadniczym celem Stowarzyszenia jest wspieranie idei samorządu terytorialnego oraz wspieranie rozwoju społeczno-gospodarczego metropolii. Głównym dokumentem strategicznym Stowarzyszenia jest opracowana i sukcesywnie od wielu lat wdrażana „Strategii Rozwoju Aglomeracji Poznańskiej. Metropolia Poznań 2020” – Centrum Badań Metropolitalnych w Poznaniu, 2011 (w skrócie „Strategii”). Pierwszym znaczącym rezultatem prowadzonych działań, zgodnie z założeniami „Strategii Rozwoju Aglomeracji Poznańskiej. Metropolia Poznań 2020” (oś „Gospodarka przestrzenna i środowiskowa”) było opracowanie „Koncepcji Kierunków Rozwoju Przestrzennego Metropolii Poznań” – CBM, 2016 (dalej „Koncepcji”).

Zgodnie z „Koncepcją” działania Metropolii Poznań w zakresie polityki przestrzennej zostały ukierunkowane na wsparcie procesu planowania metropolitalnego i koordynację lokalnych polityk przestrzennych. Wdrożenie „Koncepcji” oparto głównie na działaniach organizacyjnych – powołaniu Metropolitalnego Forum Planowania Przestrzennego dokonującego okresowej oceny ewaluacji i stopnia wdrożenia „Koncepcji” oraz funkcjonowaniu Metropolitalnej Komisji Planistycznej, jako ciała doradczego, którego zasadniczym zadaniem było – i jest nadal opiniowanie i ocena zgodności gminnych Studiów Uwarunkowania i Kierunków Zagospodarowania Przestrzennego (SUiKZP) z „Koncepcją”. Podstawą oceny zgodności są zdefiniowane w „Koncepcji” reguły, mające na celu nie tylko uspołnienie ustaleń planistycznych, ale również docelowe wdrożenie mechanizmów monitorowania zmian w zakresie zarządzania przestrzenią metropolii, w szczególności zmian w zakresie użytkowania terenów.

Od strony praktycznej zmiany takie można monitorować prawie na bieżąco, jednak pod warunkiem, iż działania w tym zakresie we wszystkich jednostkach terytorialnych w ramach procedur administracyjnych i procesów planistycznych wsparte byłby przez zestandaryzowane rozwiązania informatyczne. Niestety nie jest to możliwe wskutek – z jednej strony braku standaryzacji procesów planistycznych – a z drugiej wskutek znaczącego zróżnicowania informatyzacji jednostek terytorialnych SMP, zwłaszcza gmin, które „odstają” od rozwiązań i technologii Miasta Poznań oraz i w większości korzystają z prostych, ewidencyjnych systemów informacji przestrzennej (firmy GEO-SYSTEM np. <https://czerwolak.e-mapa.net/>).

Problem informatyzacji, dostępu do wiarygodnej metropolitalnej informacji zarządczej dostrzeżono już w „Strategii Rozwoju Aglomeracji Poznańskiej. Metropolia Poznań 2020” (CBM, 2011) w Programie 5.3 pn. „Metropolitalny system informacyjny”, gdzie wyraźnie wskazano, iż do „pełnego wykorzystania możliwości oferowanych przez nowe technologie (informacyjne) niezbędna jest daleko idąca informatyzacja” i „integracja informatyczna wszystkich jednostek administracji publicznej działających na terenie aglomeracji, która powinna umożliwić przepływ informacji oraz kompatybilność używanych systemów w zakresie gromadzenia i przetwarzania danych, w tym danych przestrzennych, umożliwiając „koordynację informacji przestrzennej”.

W obszarze gospodarki przestrzennej w „Strategii” wskazano na występujące w metropolii trudności, wynikające z braku integracji dokumentów planistycznych z danymi analitycznymi i źródłowymi, co utrudnia „rozpoznanie skali i dynamiki procesów urbanizacji, zmian w formach użytkowania terenu oraz monitorowanie zagadnień strategicznych”.

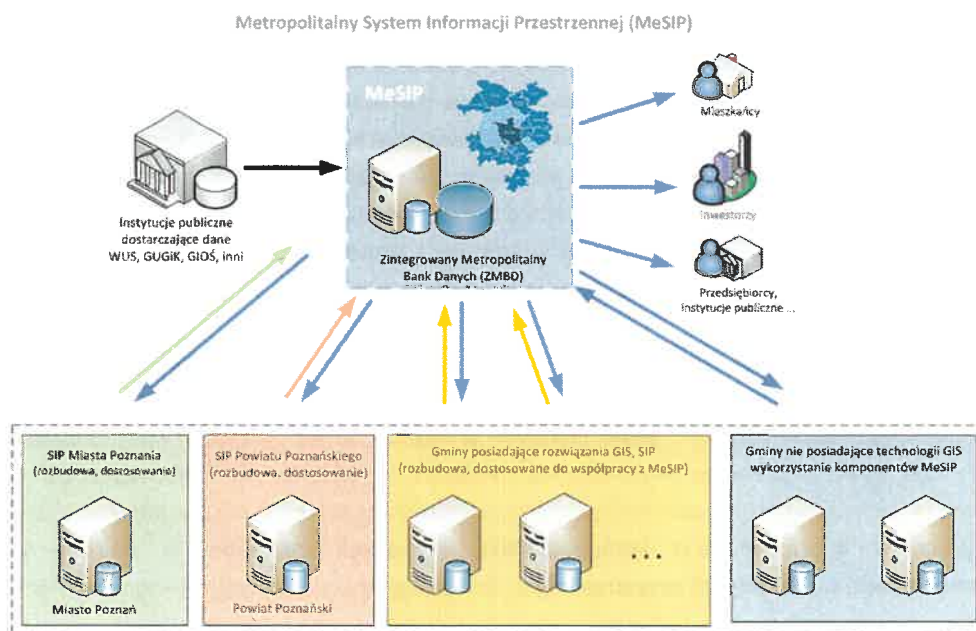
„Wizja sukcesu” programu 5.3 Strategii – to „wyraźne zwiększenie efektywności procesów decyzyjnych” i „bardziej skuteczne zarządzanie przestrzenią metropolii” dzięki wdrożeniu „kompleksowego systemu informacji o terenie, sprzężonego z dokumentami planistycznymi gmin”, wspartego „spójnym systemem wymiany danych” obejmującym „wszystkie instytucje publiczne ważne dla rozwoju metropolii”. W tak powstałym systemie powinien „funkcjonować ... zintegrowany metropolitalny bank danych, dzięki któremu pozyskiwanie informacji społeczno-gospodarczych i środowiskowych stanie się znacznie łatwiejsze”, zapewniając dostęp do wiarygodnej, aktualnej „informacji zarządczej”.

Natomiast problem partycypacji społecznej w procesach planistycznych zostanie rozwiązany poprzez uruchomienie „rozbudowanej, internetowej platformy komunikacji społecznej”, która zapewni „mieszkańcom dostęp do zintegrowanej informacji publicznej”.

Przyjęto, iż osiągnięcie celów programu „Metropolitalny system informacyjny” nastąpi poprzez połączenie sześciu działań, z których kluczowe dla koordynacji polityk przestrzennych są silnie ze sobą powiązane następujące działania:

1. Integracja informatyczna instytucji publicznych w metropolii;
2. Stworzenie metropolitalnego systemu informacji przestrzennej;
3. Budowa metropolitalnej platformy informacji publicznej i komunikacji społecznej;
4. Koordynacja pozyskiwania i wymiany danych.

Tak zdefiniowane działania z punktu widzenia „dobrych praktyk” budowy i wdrażania systemów informatycznych zostały wpisane w jedno wspólne działanie - „Budowy Metropolitalnego Systemu Informacji Przestrzennej (w skrócie MeSIP) „ - wieloinstytucjonalnego i interdyscyplinarnego systemu informatycznego, wg. „Strategii” - kompleksowego systemu informacji o terenie, wspierającego cele Metropolii Poznań w zakresie zintegrowanego zarządzania przestrzenią na każdym szczeblu jej funkcjonowania, zapewniającego wsparcie dla realizacji zadań ustawowych, w szczególności w obszarze gospodarki przestrzennej i polityk sektorowych. Ogólny ideogram systemu MeSIP przedstawia poniższy rysunek.



Rysunek 1 Ideogram MeSIP – koncepcja współdziałania systemów informatycznych jednostek terytorialnych Metropolii Poznań

4 Dodatek nr 2 - Studium wykonalności projektu

Studium wykonalności projektu „Budowa Metropolitalnego Systemu Informacji Przestrzennej (MeSIP) dla Metropolii Poznań”, w skrócie Studium Wykonalności, stanowi integralną część niniejszej specyfikacji. Studium Wykonalności dołączono do SWZ w pliku o nazwie: StudiumWykonalnosc_MeSIP.PDF.

4.1 Minimalny zakres „Wsparcia technicznego”

Zgodnie ze Studium Wykonalności pierwotny zakres „Wsparcia technicznego” powinien objąć, jako minimum:

1. Wsparcie techniczne w zakresie opisu funkcjonalnego komponentów MeSIP.
2. Nadzór nad przeprowadzeniem testów użyteczności (UX - User experience) dla każdego z modułów systemu, co powinno zapewnić przełożenie wyników badań na szczegółowe zalecenia projektowe.
3. Uczestniczenie w spotkaniach roboczych z udziałem dostawcy, wykonawcy systemu MeSIP.
4. Odbiór dokumentacji analitycznej zawierającej, co najmniej:
 - dokument inicjujący projekt,
 - dokumenty analizy przedwdrożeniowej, w tym ramowy planów testów,
 - model architektury korporacyjnej,
 - opis funkcjonalności prototypu systemu.
5. Odbiór harmonogramu prac i planu testów.
6. Odbiór prototypu systemu.
7. Odbiór komponentów dziedzinowych.
8. Odbiór środowiska testowego systemu.
9. Odbiór przeprowadzonych testów akceptacyjnych i odbiór raportu z testów.
10. Audyt bezpieczeństwa / Audyt kodu / Testy penetracyjne.
11. Audyt kodu źródłowego.
12. Testy penetracyjne.
13. Audyty bezpieczeństwa infrastruktury (sieci, urządzeń).
14. Audyt bezpieczeństwa portali MeSIP oraz aplikacji WWW.
15. Ocenę bezpieczeństwa Informacji, Polityki bezpieczeństwa informacji (elementy ISO 27001), w tym spełnienie wymagań prawnych nałożonych przez ustawodawcę w zakresie wypełnienia wymagań: KRI, ustawy o cyberbezpieczeństwie, przepisów dot. ochrony danych osobowych.
16. Odbiór oprogramowania w zakresie:
 - przekazania kodów źródłowych do oprogramowania dedykowanego,
 - przekazania licencji do oprogramowania standardowego,
 - przekazania dokumentacji do wytworzonego oprogramowania,
 - przekazania dokumentacji zawierającej konfigurację oprogramowania standardowego oraz dedykowanego,
17. Odbiór końcowy wdrożenia produkcyjnego, w tym raportu końcowego:
 - przeprowadzenie pozytywnych testów automatycznych, wydajnościowych i obciążeniowych.
18. Odbiór dokumentacji powykonawczej systemu MeSIP:
 - dane konfiguracyjne, skrypty i instrukcje,
 - kody źródłowe,
 - specyfikacja procesu integracji.

Docelowy zakres „Wsparcia technicznego” w zakresie zobowiązań i odpowiedzialności Wykonawcy po rozwinięciu ww. podstawowych tez zawiera niniejszy dokument.

5 Dodatek nr 3 - Infrastruktura Techniczna Zamawiającego, dostępne dla Wykonawcy zasoby systemowe

5.1 Charakterystyka Infrastruktury Teleinformatycznej

Na potrzeby realizacji zamówienia, Zamawiający zapewni Wykonawcy niezbędną infrastrukturę serwerową, infrastrukturę sieciową, teleinformatyczną oraz licencje oprogramowania systemowego, bazodanowego, narzędziowego, które mogą zostać wykorzystane do utworzenia środowiska narzędziowego do testów oraz audytu.

5.1.1 Zasoby dostępne dla Wykonawcy na potrzeby prowadzenia audytu oraz niezależnych testów

Z uwagi na ograniczone zasoby techniczne, po podpisaniu umowy Zamawiający wraz z Wykonawcą ustalą niezbędne zasoby techniczne jakie Zamawiający udostępni Wykonawcy do realizacji zamówienia. Zależnie od wydajności rozwiązania oferowanego przez Wykonawcę oraz rosnących potrzeb Zamawiający może zwiększyć parametry techniczne, o ile pozwolą na to warunki licencyjne produktów używanych przez Wykonawcę do implementacji oferowanego rozwiązania oraz aktualne uwarunkowania funkcjonowania całości infrastruktury technicznej Zamawiającego.

5.1.2 Wymagania dotyczące instalacji i administrowania maszynami wirtualnymi

1. Zakres zobowiązań Wykonawcy w każdej części zamówienia obejmuje czynności instalacji oraz konfiguracji dostarczanego i wdrażanego przez Wykonawcę oprogramowania. Z tego zakresu zobowiązań Zamawiający wyłącza czynności konfiguracji maszyn wirtualnych (VM), jakie będą niezbędne do realizacji zamówienia.
2. W związku z powyższym dla każdej konfiguracji VM parametry do niej muszą być szczegółowo opisane przez Wykonawcę i przekazane do Zamawiającego w formie pisemnej w formie specyfikacji przekazanej drogą elektroniczną, zgodnie z przyjętymi zasadami komunikacji.
3. Podobne ograniczenia występują w czynnościach administrowania, gdzie administrowanie maszynami wirtualnymi jest wyłącznie w gestii Zamawiającego, a czynności zarządzania konfiguracją na poziomie systemowym, narzędziowym, bazodanowym, aplikacyjnym są po stronie zobowiązań Wykonawcy.
4. W każdym przypadku, kiedy niezbędne będzie podjęcie czynności związanych z administrowaniem lub konfiguracją maszyny wirtualnej, Wykonawca jest zobowiązany skontaktować się z Zamawiającym, który te czynności wykonywać będzie bez zbędnej zwłoki.
5. Zasady współdziałania Wykonawcy i Zamawiającego w zakresie wskazanym powyżej powinny być uszczegółowione i uzgodnione przez Strony na etapie opracowania Planu Wsparcia.
6. Zakres zobowiązań Zamawiającego nie może wykraczać poza zakres zobowiązań określony w niniejszej specyfikacji oraz we wzorze umowy.

5.1.3 Zapewnienie zdalnego dostępu do Infrastruktury Technicznej

1. Zamawiający może zapewnić Wykonawcy zdalny dostęp do jego Infrastruktury Technicznej celem realizacji przez niego przedmiotu zamówienia pod następującymi warunkami: dostęp dla Wykonawcy możliwy będzie wyłącznie po podpisaniu przez Wykonawcę oświadczenia o zapewnieniu podczas realizacji zamówienia zasad określonych przez obowiązującą w organizacji Zamawiającego Politykę Bezpieczeństwa Informacji (PBI), przy uwzględnieniu, iż:



- 1.1. Zdalny dostęp do Infrastruktury Technicznej poprzez łącze VPN posiadać będzie wyłącznie określona liczba osób podana w przekazanym i zaakceptowanym przez Zamawiającego wykazie osób: /imię/nazwisko/e-mail/tel/firma – o ile jest to podwykonawca;
- 1.2. Dostęp będzie realizowany na żądanie lub w trybie określonym przez harmonogram ustalonych „okien czasowych”;
- 1.3. Dostęp do zasobów będzie realizowany poprzez VPN poprzez konta imienne aktywowane w oparciu o harmonogram;
- 1.4. Naruszenie przez Wykonawcę przyjętych przez niego zasad dostępu może skutkować stałym lub czasowym zablokowaniem dostępu zdalnego.



6 Dodatek nr 4 – Wybrane pojęcia, definicje

Nazwa	Definicja
Analiza ryzyka (systemu teleinformatycznego)	Analiza i ocena – zagrożeń, zdarzeń polegających na wykorzystaniu lub zaistnieniu podatności systemu teleinformatycznego przetwarzającego dane.
Anonimizacja	Przekształcenie danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej albo, jeżeli przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań (art. 3 pkt 1 ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, Dz. U. 2020 Nr 158 t.j.). Anonimizacja pozwala na trwałe (nieodwracalne) usunięcie powiązań między danymi osobowymi, a osobą, której dotyczą. W ten sposób informacje, które były danymi osobowymi, przestają nimi być (odwrotność pseudonimizacji).
Aplikacja	Wydzielona część systemu przetwarzającego dane realizująca cel biznesowy, zapewniająca ustalony zakres funkcjonalny dla użytkownika.
Audyt	Systematyczna i niezależna ocena danej organizacji, systemu, procesu, projektu lub produktu. Audyt dzielimy ze względu na osobę/podmiot wykonującą/y – na wewnętrzny lub zewnętrzny.
Audyt bezpieczeństwa systemu teleinformatycznego	Niezależny przegląd i ocena systemu przetwarzania danych w celu weryfikacji, przetestowania adekwatności zastosowanych środków nadzoru systemu, upewnienia się, czy system działa zgodnie z ustaloną polityką bezpieczeństwa, procedurami operacyjnymi, w tym dokumentacją systemu w celu wykrycia przełamań bezpieczeństwa i wydania zaleceń dotyczących środków nadzorowania, polityki bezpieczeństwa oraz w stosunku do procedur.
Baza danych	Zbiór powiązanych ze sobą logicznie danych, zaprojektowany dla zaspokojenia potrzeb informacyjnych organizacji w określonym zakresie dziedzinowym objętym funkcjonowaniem dziedzinowego systemu teleinformatycznego.
Dokument elektroniczny	Zgodnie z definicją zawartą w Art. 3 pkt. 2) Ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 670 z późn. zm.), inaczej – Uoinf to – stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych.
Elektroniczna usługa publiczna, inaczej e-usługa	Na podstawie dyrektywy 77/388/EWG z 2005 roku art. 9 ust. 2 lit. e) / załącznik L dyrektywy: Usługa, która jest świadczona drogą elektroniczną za pomocą sieci Internet, której wykonanie z jednej strony jest w określonym zakresie zautomatyzowane i wymaga tylko niewielkiego udziału człowieka, (jako usługobiorcy), a z drugiej strony w takim zakresie, w jakim jest świadczona – wykonanie jej bez technologii informatycznej jest niemożliwe.
Etap	Zdefiniowany, spójny ciąg działań związany z realizacją określonego zadania / zamówienia (tutaj Wykonawcy usług „Wsparcia technicznego”)
Formularz elektroniczny	Uoinf Art. 3 pkt. 25) formularz elektroniczny – graficzny interfejs użytkownika wystawiany przez oprogramowanie służący do przygotowania i wygenerowania dokumentu elektronicznego zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego.
Geoportal (lub portal mapowy)	Aplikacja sieciowa w formie portalu internetowego z graficznym interfejsem umożliwiającym dostęp do danych przestrzennych za pośrednictwem przeglądarki internetowej.

Nazwa	Definicja
Iteracja	Wielokrotne, policzalne powtórzenie jednostki zachowania w ramach określonych czynności.
Infrastruktura Techniczna Zamawiającego	Sprzęt komputerowy (serwery, macierze, urządzenia aktywne i pasywne oraz pozostałe elementy instalacyjno – konfiguracyjne infrastruktury teleinformatycznej) jak również Oprogramowanie: Aplikacyjne, Systemowe, Narzędziowe, Bazodanowe, będące w zakresie użytkowania przez Zamawiającego.
Komponent	Hermetyczny, moduł lub część oprogramowania systemu informatycznego przetwarzającego dane, realizujący usługi za pośrednictwem interfejsów.
Krajowe Ramy Interoperacyjności (KRI)	Zbiór uzgodnionych definicji, wymagań, reguł architektury systemów teleinformatycznych oraz procedur i zasad, których stosowanie umożliwi współdziałanie systemów teleinformatycznych podmiotów realizujących zadania publiczne w procesach realizacji tych zadań drogą elektroniczną.
Metodyka	Zestaw pojęć, notacji, modeli formalnych, języków i sposobów postępowania służący do analizy rzeczywistości (stanowiącej przedmiot projektowanego systemu informatycznego) oraz do projektowania pojęciowego, logicznego i/lub fizycznego. Zwykle metodyka jest powiązana z odpowiednią notacją (diagramami) służącymi do zapisywania wyniku poszczególnych faz projektu, jako środek wspomagający ludzką pamięć i wyobraźnię i jako środek komunikacji w zespołach oraz pomiędzy projektantami i klientem.
Norma (specyfikacja techniczna)	Dokument przyjęty na zasadzie konsensusu i zatwierdzony przez upoważnioną jednostkę organizacyjną, ustalający zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub zmierzający do określenia i uzyskania optymalnego stopnia uporządkowania w określonym zakresie.
Oprogramowanie	Oprogramowanie Aplikacyjne, Standardowe, Bazodanowe, Narzędziowe oraz Systemowe, rozumiane łącznie jak również każde z nich z osobna zależnie od kontekstu wystąpienia.
Oprogramowanie Aplikacyjne	Oprogramowanie opracowane i dostarczone przez wykonawcę Zadania II Budowa MeSIP, stanowiące najwyższą warstwę w wielowarstwowej architekturze budowanego Systemu, do którego tenże posiada autorskie prawa majątkowe. Oprogramowanie Aplikacyjne obejmuje wszystkie opracowane przez tego wykonawcę komponenty, procedury mające jakąkolwiek postać kodu wykonywalnego lub skryptu użytego do uruchomienia i funkcjonowania Systemu.
Oprogramowanie Standardowe	Oprogramowanie wykonawcy Zadania II Budowa MeSIP, co, do którego tenże posiada autorskie prawa majątkowe lub prawa takie należą do osoby trzeciej, ale również wykonawcy Zadania II Budowa MeSIP ma do niego pełnię praw. Oprogramowanie to zostało wytworzone przed udzieleniem wykonawcy Zadania II Budowa MeSIP i stanowi zamkniętą całość w formie modułu / komponentu / biblioteki programistycznej oraz służyć będzie do budowy i Wdrożenia Systemu.
Oprogramowanie Bazodanowe	Oprogramowanie zapewniające techniczne środki do bezpiecznego gromadzenia oraz autoryzowanego dostępu i przetwarzania danych w oparciu o relacyjną, obiektową lub obiektowo – relacyjną bazę danych.
Oprogramowanie Narzędziowe	Oprogramowanie zapewniające niezbędne funkcje techniczne na rzecz budowy i Wdrożenia Systemu, stanowiące warstwę pośrednią - usługową pomiędzy Oprogramowaniem Aplikacyjnym / Standardowym a Systemowym, z wyłączeniem Oprogramowania Bazodanowego.

Nazwa	Definicja
Oprogramowanie Systemowe	Oprogramowanie zapewniające podstawowe funkcje systemowe umożliwiające funkcjonowanie infrastruktury sprzętowej zgodnie z jej przeznaczeniem. W skład tego oprogramowania wchodzi: oprogramowanie do wirtualizacji oraz systemy operacyjne.
Podatność	Słabość lub luka w systemie przetwarzania danych. Wady lub luki w strukturze fizycznej, organizacji, procedurach, zarządzaniu, administrowaniu, sprzęcie, oprogramowaniu, a także zmierzone i niezmierzone działania personelu, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika
Przypadek użycia	Opis wymagań wobec systemu teleinformatycznego przedstawiający interakcję pomiędzy „aktorem”, który inicjuje zdarzenie oraz opisywanym systemem – zdefiniowany przez opis, sekwencji prostych kroków. Przypadek użycia może być przedstawiony graficznie w formie tzw. diagramu przypadków użycia. Uogólniając przypadek użycia może odnosić się do zachowania Obiektu w osiągnięciu określonego stanu.
Przypadek testowy	Ścisłe określona „ścieżka przejścia” w ramach procedury testowej prowadzonej zgodnie z planem testów odnosząc się do określonego scenariusza zachowania testowanego produktu lub charakterystycznej klasy danych wejściowych. Kluczowe dla właściwego określenia przypadku testowego jest jednoznaczne określenie oczekiwanego, spodziewanego wyniku wykonania procedury testowej.
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (RODO). Zalecane techniki pseudonimizacji zawarte w opinii 05/2014 wydanej przez Grupę Roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (RODO Art. 29) to: szyfrowanie z kluczem; funkcje hash tzw. funkcje skrótu, zastosowanie tokena.
RODO	Rozporządzenie 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 – tzw. ogólne rozporządzenie o ochronie danych.
Rejestr publiczny	Uoinf Art. 3 pkt. 5) rejestr publiczny – rejestr, ewidencję, wykaz, listę, spis albo inną formę ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie odrębnych przepisów ustawowych.
Schemat aplikacyjny	Schemat pojęciowy dla danych wykorzystywanych przez jedną lub więcej aplikacji.
System	W skrócie system teleinformatyczny MeSIP
System teleinformatyczny	Uoinf Art. 3 pkt. 3) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r., poz.576 t.j.).
Testy akceptacyjne	Przeprowadzenie procedury testowej sprawdzającej dla określonej części systemu weryfikującej zgodność wyników testów z wartością oczekiwaną oraz ze specyfikacją. Testy akceptacyjne są realizowane przez Zamawiającego.

Nazwa	Definicja
	Pozytywne wyniki testów w zakresie ustalonym w Planie Testów stanowi podstawę do odbioru.
Testy bezpieczeństwa	Testy sprawdzające podatność oraz poprawność i skuteczność funkcjonowania zabezpieczeń oprogramowania. Zabezpieczenia są to środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko. Wynika z tego, że testowaniu podlegają zarówno zabezpieczenia typowo informatyczne, ale także zabezpieczenia fizyczne i inne.
Testy funkcjonalne	Testy sprawdzające zgodność ze specyfikacją lub dokumentacją techniczną w zakresie wymagań funkcjonalnych testowanego oprogramowania.
Testy integracyjne – komunikacji	Testy poprawności powiązań między modułami / usługami oraz systemami zewnętrznymi
Testy niefunkcjonalne	Testy sprawdzające zgodność ze specyfikacją lub dokumentacją techniczną w zakresie parametrów i cech niefunkcjonalnych testowanego oprogramowania.
Testy penetracyjne	Testy polegające na autoryzowanej „siłowej” próbie oceny bezpieczeństwa infrastruktury teleinformatycznej. Testy penetracyjne można nazwać etycznym hackingiem.
Testy regresyjne	Testy regresyjne wersji systemu są to testy sprawdzające, czy funkcjonalność poprzedniej wersji systemu działa prawidłowo w aktualnej wersji. Testy te występują najczęściej podczas utrzymywania systemu i rozszerzania jego funkcjonalności. Automatyzacja tego rodzaju testów jest szczególnie wskazana ze względu na możliwości pełnego wykonania testów.
Testy użyteczności	Testy sprawdzające cechy użytkowe oprogramowania na zgodność ze specyfikacją lub dokumentacją techniczną w tym zakresie.
Testy wydajnościowe	Testy sprawdzające zgodność ze specyfikacją lub dokumentacją techniczną w zakresie parametrów wydajnościowych systemu lub jego części – stanowią część testów akceptacyjnych lub weryfikacyjnych prowadzonych przez podmiot trzeci.
Testy black box	Rodzaj testów. Testy te zakładają, że jest znana specyfikacja systemu natomiast nie jest istotna znajomość konstrukcji wnętrza systemu. Nastawione są na poszukiwanie niezgodności implementacji ze specyfikacją. Dane wejściowe i oczekiwane wyniki przygotowywane są na podstawie specyfikacji. Podczas testów system jest traktowany jak czarna skrzynka, na wejściu której podajemy przygotowane dane wejściowe i sprawdzamy, czy otrzymane wyniki zgadzają się z oczekiwanymi. Testy te mają szerokie zastosowanie począwszy od testów wewnętrznych - jednostkowych prowadzonych przez autora / dostawcę oprogramowania dla poszczególnych funkcji, aż po testy całego systemu.
Testy gray box	Rodzaj testów. Testy łączące cechy testów black box i white box, z uwagi na brak pełnej wiedzy nt. działania testowanego komponentu oprogramowania.
Testy white box	Rodzaj testów. Testy te zakładają znajomość konstrukcji systemu. Nastawione są na poszukiwanie błędów związanych ze złą konstrukcją programu (nieprawidłowe wykorzystanie pętli, instrukcji warunkowych, instrukcji operacji na bazie danych itp.). Testy te mają zastosowanie szczególnie w testach jednostkowych lub w przypadku dostępności kodów źródłowych oprogramowania.
Usługi (publiczne)	Usługi świadczone przez organy administracji publicznej dla obywateli, podmiotów gospodarczych oraz organizacji, a także inne formy komunikacji pomiędzy organami administracji publicznej a obywatelami i organizacjami, służące realizacji zadań administracji publicznej lub wywiązywaniu się obywateli i organizacji z obowiązków wobec państwa

Nazwa	Definicja
Usługa danych przestrzennych (ang. spatial data services)	Usługa będąca operacjami, które mogą być wykonywane przy użyciu oprogramowania komputerowego na danych zawartych w zbiorach danych przestrzennych lub na powiązanych z nimi metadanych.
Usługa sieciowa	Komponent / część oprogramowania, realizujący określone funkcje logiki Systemu. Komponent może być wywołany zdalnie poprzez zdefiniowany interfejs.
Wzór dokumentu elektronicznego	Uoinf Art. 3 pkt. 24) wzór dokumentu elektronicznego – zbiór danych określających zestaw, sposób oznaczania oraz wymagalność elementów treści i metadanych dokumentu elektronicznego, a także mogących określać sposób zapisu danych dla wskazanych elementów oraz kolejność i sposób wyświetlania na ekranie lub drukowania poszczególnych elementów (wizualizacji).

Opis przedmiotu zamówienia sporządzili:

Marek Stawarz

Julita Niedroślańska

Bartosz Błaszczuk

Kierownik Wydziału
Systemu Informacji Przestrzennej


Marek Stawarz

DYREKTOR
GEODETA POWIATOWY


Tomasz Powroźnik

Główny Specjalista


Julita Niedroślańska

Starszy Referent

Bartosz Błaszczuk