Załącznik nr 1
numer sprawy: CIS-WAG.271.10.2017

**Opis Przedmiotu Zamówienia**

***Słowniczek skrótów użytych w Opisie Przedmiotu Zamówienia***

CIS – Centrum informatyki Statystycznej
ESS – Europejski System Statystyczny
GUS – Główny Urząd Statystyczny,
OBM – Operacyjna Baza Mikrodanych,
UE – Unia Europejska.

## I. Tło akcji

W 2015 r. Eurostat i wybrane państwa członkowskie przeprowadziły w ramach podprojektu SIMSTAT próbną wymianę mikrodanych z handlu zagranicznego pochodzących z INTRASTAT (w GUS są to dane pochodzące z Ministerstwa Finansów).

Celem SIMSTAT była próbna wysyłka mikrodanych statystycznych. Wysyłka danych z GUS była przeprowadzona przez komponent SIMSTAT dostarczony przez Eurostat przy użyciu bramki CCN. Projekt SIMSTAT został zakończony sukcesem. Obecnie wymiana danych nie jest prowadzona.

Eurostat planuje w ramach ESS rozpocząć od 2020 r. wymianę mikrodanych z handlu zagranicznego używając systemu ESDEN. Dane z MF o wywozie towarów z Polski będą wysyłane przez GUS wraz z ID partnera zagranicznego (towar od partnera X <polskiego> do partnera Y z kraju członkowskiego w ujęciu miesięcznym). Dane będą wysyłane przez Hub Eurostatu do innych państw członkowskich. Dane innych państw będą przysyłane do GUS.

W celu umożliwienia realizacji połączenia Eurostat zaplanował szereg działań, w tym realizację grantu na podłączenie Państw członkowskich do sieci gov.net i TESTA; opracowanie portalu EDAMIS4 w ramach ESDEN dedykowanego do wysyłania danych (komponent dostarczany przez Eurostat); szereg działań wspierających na poziomie merytorycznym (charakter wymienianych danych) i organizacyjnym.

Dane planowane do wymiany mają różny poziom zabezpieczeń zależnie od wymagań prawnych Państwa członkowskiego. ESSC (Komitet Sterujący ESS) w maju 2016 r. przyjął dokument „Wspólne ramy bezpieczeństwa IT ESS" (IT Common Security Framework lub IT Security Framework) określający jednolity standard zabezpieczeń dla wszystkich państw członkowskich. Dokument został przygotowany na podstawie rodziny norm ISO/IEC 27000 i jest z nim w pełni zgodny.

Wymiana danych z handlu zagranicznego została wpisana do aktualnie procedowanego dokumentu FRIBS (Framework regulation integrating business statistics) jako obowiązkowa od 2020 r.

Eurostat zaplanował certyfikację wszystkich państw członkowskich i Eurostatu, wykonaną przez zewnętrznego audytora. Certyfikacja jest ograniczona do zakresu mikrodanych z

handlu zagranicznego wymienianych z Eurostatem. GUS/CIS został zgłoszony do certyfikacji w 2019 r.

W marcu 2017 r. Zamawiający otrzymał dotację z Eurostatu na:

1. Napisanie i wdrożenie szeregu polityk, standardów, wytycznych i procedur zgodnych z przedstawionym frameworkiem.
2. Wdrożenie systemu zbierającego logi.
3. Usługę wykonania audytu środowiska po realizacji grantu.

Niniejsze zamówienie ma na celu realizację punktu 1 ww. grantu.

## II. Cel zamówienia

Celem realizacji zamówienia jest podniesienie bezpieczeństwa IT w obszarze wymiany poufnych danych statystycznych zgodnie z wymaganiami Wspólnych Ram Bezpieczeństwa IT Europejskiego System Statystycznego.

Cel zostanie osiągnięty przez napisanie i wdrożenie wybranych polityk, standardów, wytycznych i procedur wspierających Politykę bezpieczeństwa informacji dla obszaru mikrodanych statystycznych wymienianych obowiązkowo między Eurostatem a Rzeczpospolitą Polską lub między Państwami członkowskimi.

Cel ten zostanie zrealizowany przez analizę obecnego środowiska wymiany i wykorzystania danych z handlu zagranicznego (etap I), opracowanie projektu docelowego środowiska informatycznego dla wymiany danych oraz analiz (etap II), opracowanie dokumentacji bezpieczeństwa dla docelowego środowiska zaprojektowanego w etapie II (etap III).

Rezultatem zamówienia powinny być powstałe i przyjęte wybrane polityki, standardy, wytyczne zgodnie z rolami i zakresem odpowiedzialności w organizacji określonymi w obowiązującej Polityce Bezpieczeństwa Informacji.

Polityki, standardy i wytyczne będą utrzymywane w pracy operacyjnej organizacji przez uprawnionych pracowników Centrum Informatyki Statystycznej i Biura Zarzadzania Bezpieczeństwem Informacji GUS. Zostaną poddawane przeglądom, będą monitorowane i rozwijane wg metody zaproponowanej przez Eurostat w ESS Core IT Security Framework, tj.: Planuj– Wykonuj – Sprawdzaj – Działaj.

## III. Przepływ danych

1. Płyta CD z danymi pochodzącymi z systemu INTRASTAT z Ministerstwa Finansów jest przesyłana raz w miesiącu.
2. Zbiory z płyty trafiają do dwóch baz:

   - OBM – to baza, w której m.in. prowadzone są prace na zbiorach danych z zewnętrznych systemów informacyjnych. W bazie tej dane z zewnętrznych systemów informacyjnych są przekształcane w dane statystyczne, jak również przetwarzane w zakresie wyliczania dodatkowych zmiennych, wyodrębniania podzbiorów i łączenia zbiorów. Zbudowany System Operacyjnej Bazy Mikrodanych obejmuje infrastrukturę

sprzętowo-systemowo-narzędziową (sprzęt komputerowy, oprogramowanie systemowe, oprogramowanie narzędziowe) oraz oprogramowanie aplikacyjne (programy komputerowe będące efektem prac programistycznych Wykonawcy systemu). Baza wykorzystuje narzędzia bazodanowe MS SQL i analityczne SAS,

- Baza produkcyjna na serwerze bazodanowym MS SQL, w której dokonywane są analizy danych, m.in. scalanie danych z danymi z innych systemów. Liczba użytkowników wynosi nie więcej niż 15 osób. Dane z obszaru handlu zagranicznego są automatycznie zaciągane do repozytorium danych statystycznych i następnie po sprawdzeniu do hurtowni danych.

3. Dla pilotażu SIMSTAT kolejnym etapem było przygotowanie mikro-danych w postaci pliku CSV, który poprzez udostępniony folder trafiał do osoby odpowiedzialnej za wysłanie danych. Dane były wysyłane i odbierane przy użyciu VPN i dostarczonego przez Eurostat komponentu komunikacji SIMSTAT.

4. Docelowo wymiana danych nastąpi poprzez dostarczony przez Eurostat system Edamis przy użyciu gov.net / TESTA. Podłączenie zostanie wykonane w ramach grantu z Eurostatu. Docelowo łącze powinno przesyłać dane na wydzielony komputer. Odseparowanie jest wymaganiem operatora usługi. Z ISODS dane powinny być przekazywane do systemów produkcyjnych przy pomocy zewnętrznych nośników danych (płyta lub inne).

## IV. Wymagania dla etapu I - Analiza obecnego środowiska wymiany i przetwarzania danych z handlu zagranicznego

Dokument „Analiza obecnego środowiska wymiany i wykorzystania danych z handlu zagranicznego” musi:

1. Zawierać analizę otoczenia wewnętrznego i zewnętrznego w zakresie wykorzystywania danych z handlu zagranicznego pochodzących z INTRASTAT, w tym szczególnie:
    a) workflow zgodnie z rozdziałem III;
    b) schemat przepływu danych;
    c) analizę techniczną funkcjonalności i usług wykorzystywanych systemów;
    d) analizę otoczenia prawnego z zakresu regulacji dot. bezpieczeństwa informacji;
    e) opis relacji między wykorzystywanymi systemami a rodziną norm ISO 27000,w tym szczególnie opis relacji między wykorzystywanymi systemami a politykami, wytycznymi i standardami określonymi w Etapie III.
2. Zawierać analizę interesariuszy.
3. Definiować potrzeby wewnętrznych i zewnętrznych odbiorców projektu.
4. Zawierać analizę problemów i analizę ryzyka.

5. Proponować co najmniej dwa rozwiązania, z których jedno będzie podstawą do opracowania Projektu technicznego, o którym mowa w Etapie II. W tej części dokument musi zawierać w obydwu wariantach:

    a) analizę porównawczą funkcjonalności obecnie wykorzystywanych systemów z funkcjonalnościami proponowanymi, uwzględniającą istniejące rozwiązania i systemy informatyczne Zamawiającego oraz ich wzajemne powiązania;

    b) analizę zasadności realizacji projektu ze względu na potrzeby interesariuszy;

    c) analizę kosztów;

    d) zakres projektu oraz jego kluczowe parametry,

    e) wskazywać najkorzystniejszy wariant realizacji projektu,

    f) oszacowanie nakładów inwestycyjnych i utrzymania rezultatów,

    g) harmonogram realizacji.

## V. Wymagania dla etapu II - Opracowanie projektu technicznego docelowego środowiska informatycznego dla wymiany danych oraz analiz

Projekt techniczny będzie opisywał docelowe środowisko wymiany i przetwarzania danych z handlu zagranicznego pochodzących z systemu INTRASTAT.

Projekt techniczny musi:

1. Określać zakres projektu oraz jego kluczowe parametry, w tym zawierać:

    a) opracowanie wniosków na podstawie przeglądu obecnego systemu informatycznego (Etap I).

    b) opracowanie koncepcji nowego systemu informatycznego, z uwzględnieniem architektury systemu.

    c) opis niezbędnej infrastruktury systemu z uwzględnieniem infrastruktury zamawiającego.

    d) opracowanie analizy potrzeb i metody integracji systemu z systemami związanymi.

    e) konfigurację poszczególnych komponentów oraz usług.

    f) konfiguracja oprogramowania na stacji roboczej.

    g) zasady administrowania definiujące role dla pracowników wraz z delegacją uprawnień.

2. Określać cele projektu.

3. Zawierać harmonogram realizacji projektu określający sekwencje i zależności miedzy zadaniami oraz czas potrzebny na przeprowadzenie wszystkich niezbędnych zadań, jak również określający kamienie milowe.

4. Opisywać środowisko zapewniające bezpieczeństwo danych wg ISO27000 i zaspokajać potrzeby biznesowe użytkowników.

## VI. Wymagania dla etapu III - Opracowanie dokumentacji bezpieczeństwa dla docelowego środowiska zaprojektowanego w etapie II

1. W etapie IIII wykonawca opracuje i przedstawi Zamawiającemu 49 dokumentów:

| | Nazwa polska | Nazwa angielska | Docelowy zakres wdrożenia |
|---|---|---|---|
| | **Polityki tematyczne:** | **Thematic policies:** | |
| 1 | Polityka akceptowalnego wykorzystania aktywów | Information asset acceptable use policy | Organizacja |
| 2 | Polityka postępowania z nośnikami | Removable media governance policy | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 3 | Polityka przekazywania nośników | Physical media transfer policy | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 4 | Polityka kontroli dostępu | Access control policy | Organizacja |
| 5 | Polityka stosowania poufnych informacji uwierzytelniających | Secret authentication information handling policy | Organizacja |
| 6 | Polityka zabezpieczenia kryptograficznego | Cryptographic policy | Organizacja |
| 7 | Polityka zarządzania kluczami kryptograficznymi | Cryptographic key lifecycle policy | Organizacja |
| 8 | Polityka ponownego użycia zasobów | Asset reused policy | Organizacja |
| 9 | Polityka czystego biurka | Clear desk policy | Organizacja |
| 10 | Polityka czystego ekranu | Clear screen policy | Organizacja |
| 11 | Polityka przysyłania informacji | Information transfer policy | Organizacja |
| 12 | Polityka przysyłania wiadomości elektronicznych | Electronic messaging systems acceptable use policy | Organizacja |
| 13 | Polityka bezpieczeństwa prac rozwojowych | Secure development policy | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 14 | Polityka zmian w pakietach oprogramowania | Software packages manipulation acceptable use policy | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 15 | Polityka gromadzenia materiału dowodowego | Forensic readiness policy | Organizacja |
| 16 | Polityka ochrony zapisów | Data protection security policy | Organizacja |
| | **Standardy**: | **Standards:** | |
| 17 | Standardy kontroli dostępu do | Role base access control | SIMSTAT i inne środowiska |

| | | | |
|---|---|---|---|
| | sieci i usług sieciowych | standard | wykorzystujące dane z SIMSTATu |
| 18 | Standardy zabezpieczeń kryptograficznych | Cryptographic standard | Organizacja |
| 19 | Standardy zarządzania zmianą | Change management standard | Organizacja |
| 20 | Standardy zarządzania pojemnością | Capacity management standard | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 21 | Standardy wykrywania szkodliwego oprogramowania | Malware detection standard | Organizacja |
| 22 | Standardy odzyskiwania zainfekowanego oprogramowania | Malware infection and capacity recovery standard | Organizacja |
| 23 | Standardy zarządzania ryzykiem w zakresie podatności oprogramowania | Risk assessment standard | Organizacja |
| 24 | Standardy zabezpieczenia informacji | Information protection in systems and application standard (network controls) | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 25 | Standardy bezpieczeństwa prac rozwojowych | Secure development standard | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 26 | Standardy zarządzania incydentami | Incident management standard | Organizacja |
| 27 | Standardy oceny zdarzeń związanych z bezpieczeństwem informacji | Information security events assessment standard | Organizacja |
| 28 | Standardy reagowania na incydenty związane z bezpieczeństwem informacji | Incident response standard | Organizacja |
| | **Wytyczne:** | **Guidelines:** | |
| 29 | Wytyczne dot. zwrotu aktywów | Asset return guidelines | Organizacja |
| 30 | Wytyczne dot. zarzadzania nośnikami wymiennymi | Removable media guidelines | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 31 | Wytyczne dot. przekazywania nośników | Physical media transfer guidelines | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 32 | Wytyczne dot. rejestrowania i wyrejestrowania użytkowników | User access registration guidelines | Organizacja |
| 33 | Wytyczne dot. przydzielania dostępu użytkownikom | User access provisioning guidelines | Organizacja |
| 34 | Wytyczne dot. zarzadzania poufnymi informacjami | Secret authentication information allocation | Organizacja |

| | | | |
|---|---|---|---|
| | uwierzytelniającymi użytkowników | guidelines | |
| 35 | Wytyczne dot. przeglądu praw dostępu użytkowników | Access rights review guidelines | Organizacja |
| 36 | Wytyczne dot. ochraniania lub dostosowywania praw dostępu | Access rights adjustment guidelines | Organizacja |
| 37 | Wytyczne dot. zabezpieczenia biur, pomieszczeń i obiektów | Secure areas management guidelines | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 38 | Wytyczne dot. dostępu do środowisk rozwojowych, testowych i produkcyjnych | Unauthorized changes control guidelines | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 39 | Wytyczne dot. wykrywania szkodliwego oprogramowania | Malware detection guidelines | Organizacja |
| 40 | Wytyczne dot. zapobiegania rozprzestrzeniania szkodliwego oprogramowania | Malware spreading prevention guidelines | Organizacja |
| 41 | Wytyczne dot. odzyskiwania zainfekowanego oprogramowania | Malware infection and capacity recovery guidelines | Organizacja |
| 42 | Wytyczne dot. rejestrowania zdarzeń | User activities recording guidelines | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 43 | Wytyczne dot. kontroli nad instalowanym oprogramowaniem | Software installation control guidelines | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 44 | Wytyczne dot. zabezpieczenia informacji w oprogramowaniu | Information protection in systems and applications guidelines (network controls) | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 45 | Wytyczne dot. zabezpieczenia przed nieautoryzowanym przesyłaniem informacji | Non-authorized forms of data transfer prevention guidelines | Organizacja |
| 46 | Wytyczne dot. ochrony transakcji danych | Application services transactions protection guideline | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 47 | Wytyczne dot. bezpieczeństwa prac rozwojowych | Secure development guidelines | SIMSTAT i inne środowiska wykorzystujące dane z SIMSTATu |
| 48 | Wytyczne dot. zgłaszania słabości związanych z bezpieczeństwem informacji | Information security weakness reporting guidelines | Organizacja |
| 49 | Wytyczne dot. wyciągania wniosków związanych z bezpieczeństwem informacji | Information security incidents lessons learned guidelines | Organizacja |

2. Każdy z ww. dokumentów:

    1) Będzie dokumentem uzupełniającym dla Polityki Bezpieczeństwa Informacji.

    2) Musi być opracowany na podstawie rodziny norm ISO 27000.

    3) Musi być zgodny z aktualnie wdrożonymi dokumentami w organizacji lub proponować ich zmianę. W przypadku uznania, po analizie przeprowadzonej w ramach etapu I, dotychczas wdrożonych i wykorzystywanych polityk, standardów, wytycznych lub innych dokumentów za wystraczające do realizacji celów niniejszego zamówienia, Zamawiający po weryfikacji uzna je za spełniające cel niniejszego zamówienia.

## VII. Wymagania formalne dla usług wsparcia

1. Niniejszy rozdział dotyczy wykonawcy, który zaoferował w ofercie wsparcie w Kryterium wyboru ofert „W" i którego oferta została wybrana.

2. Usługi wsparcia będą świadczone do 31 grudnia 2018 r. lub do wyczerpania limitu godzin.

3. Wykonanie wsparcia zostanie rozliczone na podstawie kwartalnych raportów, w przypadku wykorzystania usługi wsparcia w danym kwartale.

4. Usługi wsparcia obejmują:

    1) Wsparcie merytoryczne we wdrożeniu systemu powstałego w wyniku realizacji projektu technicznego w etapie II.

    2) Wsparcie merytoryczne w obszarze polityk, standardów i wytycznych w związku z:

        a) Zmianami w rodzinie norm ISO27000 wpływającymi na kształt ww. dokumentów.

        b) Zmianami uwarunkowań prawnych i regulacyjnych.

        c) Wdrożeniem systemu zaprojektowanego w etapie II.

        d) Wdrożeniem pełnym lub częściowym SZBI w GUS lub CIS.

5. Zamawiający zobowiązuje się, że nie będzie wykorzystywał więcej niż 100 godzin wsparcia miesięcznie, a Wykonawca zobowiązuje się wsparcie wykonać.

6. Zamawiający ma prawo do realizacji wsparcia w swojej siedzibie, jeżeli cel zlecenia wsparcia wymaga obecności pracownika Wykonawcy. W pozostałych pracach Zamawiający dopuszcza wszystkie formy wymiany współpracy, w tym przede wszystkim przy użyciu środków elektronicznych.

7. Dla każdego pojedynczego zlecenia wsparcia zostanie określona przez Zamawiającego liczba godzin wsparcia. W przypadku rozbieżności co do pracochłonności zlecenia liczba godzin może zostać zmieniona na podstawie oświadczenia Wykonawcy, w którym wykaże i poprze dowodami pracochłonność.

8. Od zgłoszenia zlecenia przez Zamawiającego do momentu rozpoczęcia zlecenia nie może minąć więcej niż 5 dni roboczych. Po tym okresie zlecenie uznane zostanie za opóźnione.

9. Zlecenie niezrealizowane w terminie uzgodnionym w zleceniu uznane zostanie za opóźnione. Zamawiający dopuszcza możliwość modyfikacji terminu wykonania zlecenia z uzasadnionych powodów.

10. Zamawiający dopuszcza stworzenie dokumentu bazowego, w którym przed rozpoczęciem realizacji wsparcia dla poszczególnych rodzajów zleceń zostanie określona ich bazowa pracochłonność. Dokument musi zostać uzgodniony przed podpisaniem końcowego protokołu odbioru.

11. Metoda komunikacji, kanał dostępowy, szczegółowa procedura dla wsparcia zostanie pisemnie uzgodniona z Wykonawcą przed podpisaniem końcowego protokołu odbioru.

## VIII. Wymagania formalne dla dokumentów (Etap I-III)

Wykonawca będzie zobowiązany do wykonania Przedmiotu zamówienia z należytą starannością, zgodnie z zasadami wiedzy technicznej, obowiązującymi przepisami prawa polskiego i europejskiego oraz w taki sposób, aby zastosowane rozwiązania pozwoliły na zminimalizowanie kosztów inwestycyjnych, wydatków rzeczowych, w tym eksploatacyjnych.

Dokumentacja zostanie przygotowane z uwzględnieniem następujących wymagań:

1. Będzie opracowaniem kompletnym i wyczerpującym z punktu widzenia celu, któremu ma służyć,

2. Zostanie przygotowany w języku polskim, w formie papierowej (format A-4, średnia ilość znaków na stronie – 1 900) oraz formie elektronicznej w formacie plików do edycji. Forma graficzna publikacji, czcionki, formatowanie strony, wygląd ew. ilustracji, itp. zostanie ustalona po podpisaniu umowy,

3. Lista dokumentów i materiałów źródłowych, które posłużyły Wykonawcy do sporządzenia Projektu technicznego wraz z ich zbiorem zostanie przygotowana w wersji elektronicznej.

4. W przypadku wystąpienia zmiany w obowiązujących przepisach prawnych oraz dokumentach stanowiących wytyczne i instrukcje wykonania całości przedmiotu zamówienia, Wykonawca zobowiązuje się do uwzględnienia tych zmian i dostosowania przedmiotu zamówienia bez dodatkowego wynagrodzenia w trakcie trwania umowy.

5. Wykonawca zobowiązuje się do przekazywania Zamawiającemu wszelkich informacji mających wpływ na realizację Przedmiotu zamówienia oraz do niezwłocznego udzielania odpowiedzi i wyjaśnień na zgłaszane przez Zamawiającego uwagi dotyczące jego realizacji w formie pisemnej.

6. Wykonawca dostarczy Zamawiającemu ostateczną i zaakceptowaną przez Zamawiającego wersję dokumentów, w wersji papierowej w 2 egzemplarzach oraz w wersji elektronicznej na nośniku optycznym CD lub DVD. Dokumenty zostaną dostarczone do siedziby Zamawiającego.

7. Wykonawca na każdym etapie realizacji Przedmiotu zamówienia będzie ściśle współpracował z przedstawicielami Zamawiającego, ponadto w miarę bieżących potrzeb, odbywać się będą spotkania robocze Zamawiającego z Wykonawcą.

8. Dokumentacja powinna być przygotowana jedynie na potrzeby realizacji niniejszego zamówienia.

9. Na potrzeby opracowania przedmiotu zamówienia zamawiający udostępni po podpisaniu umowy posiadane materiały i dokumenty, które mogą być pomocne przy realizacji zamówienia.

10. Wykonawca dostarczy wymagane dokumenty na nie mniej niż 3 dni robocze przez datą odbioru etapu. Szczegółowy harmonogram dostarczania dokumentów z Etapu III zostanie uzgodniony z wykonawcą po podpisaniu umowy.

## IX. Harmonogram

Wykonawca będzie zobowiązany do wykonania Przedmiotu zamówienia w poniższych terminach i w następujący sposób:

1. W terminie do 6 dni roboczych od dnia zawarcia umowy weźmie udział w spotkaniu organizacyjnym z Zamawiającym w siedzibie Centrum Informatyki Statystycznej w Warszawie. Celem spotkania będzie omówienie i uzgodnienie harmonogramu prac.
2. Termin realizacji Etapu I – do dnia 18 września 2017 r
3. Termin realizacji Etapu II – do dnia 16 października 2017 r.
4. Termin realizacji Etapu III – do dnia 16 listopada 2017 r.

## X. Odbiór Przedmiotu Zamówienia

1. Dokumentacja opracowana w ramach realizacji Przedmiotu Zamówienia weryfikowana będzie według następujących kryteriów:
   1) zawartość merytoryczna – treść dokumentu powinna zawierać informacje istotne, niosące treść adekwatną do zakresu dokumentu;
   2) zakres – treść dokumentu winna obejmować uzgodniony zakres prac, wszystkie kwestie mieszczące się w uzgodnionym zakresie muszą zostać zawarte w dokumencie;
   3) klarowność – dokument winien być tak napisany, by czytelnik był w stanie zrozumieć jego treść bez potrzeby zasięgania wyjaśnień u autora, szczególnie istotna jest struktura oraz czytelność raportów i specyfikacji, w określonych przypadkach dokument winien zawierać słowniczek używanych terminów lub inne materiały pomocnicze;
   4) precyzja – specyfikacje, opisy czy uwagi zawarte w dokumencie winny być poprawne, jednoznaczne i kompletne.
2. Wykonawca zobowiązuje się do wprowadzenia uwag lub poprawek zamawiającego w dokumentach przed datą odbioru właściwego etapu.