

## Opis Przedmiotu Zamówienia

### **Przeprowadzenie audytu bezpieczeństwa informacji dla systemu wymiany mikro danych wg wymagań Wspólnych Ram Bezpieczeństwa Europejskiego Systemu Statystycznego**

#### **I. Tło akcji**

W 2015 r. Eurostat i wybrane państwa członkowskie przeprowadziły w ramach projektu SIMSTAT próbną wymianę mikro danych z handlu zagranicznego pochodzących z systemu INTRASTAT (dane zbierane oraz kontrolowane dla celów statystyki handlu zagranicznego przez Ministerstwo Finansów, dalej jako „MF”).

Celem projektu SIMSTAT było przetestowanie zdolności państw członkowskich do wymiany mikro danych statystycznych na próbnych danych. Wymiana danych między hubem Eurostatu a GUS była przeprowadzona przez komponent SIMSTAT przy użyciu bramki CCN w Ministerstwie Finansów. Wymiana danych w projekcie SIMSTAT została zakończona sukcesem. Wymiana danych miała charakter próbny i nie jest obecnie prowadzona.

Eurostat, w ramach realizowanej obecnie Wizji ESS 2020, planuje rozpocząć od 2020 r. wymianę mikro danych dot. handlu wewnętrznego pomiędzy państwami członkowskimi. W tym celu realizowany jest projekt ESDEN (*European statistical data exchange network*). Dane dot. wywozu 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 poprzez centralny punkt (hub utworzony w Eurostat) do innych państw członkowskich. Dane innych państw będą przysyłane do GUS przez hub centralny. Wysyłane dane będą miały charakter jednostkowy. Należy zwrócić uwagę, iż charakter i struktura mikro danych nie zostały dotychczas jednoznacznie określone przez Eurostat, w związku z czym ww. cechy danych mogą ulec zmianie.

Dane przeznaczone do wymiany mają różny poziom zabezpieczeń zależnie od regulacji krajowych państw członkowskich. 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 wraz z powiązаныmi normami (w szczególności ISO/IEC 27000, 27001 i 27002). Dokument zawiera ponad 90 wymagań dotyczących bezpieczeństwa informacji. Zakres dokumentu pokrywa przede wszystkim obszar systemów teleinformatycznych i organizacyjny, w mniejszym stopniu procesów kadrowych i bezpieczeństwa fizycznego.

Wymiana mikro danych z handlu zagranicznego została wpisana do aktualnie procedowanego dokumentu FRIBS (*Framework Regulation Integrating Business Statistics*) jako obowiązkowa od 2020 r. Eurostat

planuje umożliwić fizyczną wymianę danych po weryfikacji czy dane państwo spełnia wymagania bezpieczeństwa określone w *IT Security Framework*. W związku z powyższym Eurostat zaplanował certyfikację państw członkowskich oraz Eurostatu przez zewnętrznego audytora. GUS / CIS został zgłoszony do procesu certyfikacyjnego na 2019 r.

Zakres certyfikacji określają dwa dokumenty:

- „Wspólne ramy bezpieczeństwa IT ESS” w zakresie wskazania obszarów certyfikacji, dowodów koniecznych do wykazania spełnienia wymagań oraz koniecznych przeglądów bezpieczeństwa.
- Dokument „Mitigation of risks related to the exchange of identifiable micro-data” ” stanowiący uzupełnienie powyższego dokumentu o wskazanie kontrolek bezpieczeństwa, które:
  - Mają kluczowe znaczenie w procesie certyfikacji (podział „major / minor”)
  - Mają zastosowanie do całej organizacji lub jedynie obszaru wykorzystania mikrodanych z handlu zagranicznego (ang. *Micro Data Exchange*).

## II. Cel zamówienia

Niniejsze zapytanie ofertowe ma na celu wskazanie aktualnego stanu bezpieczeństwa informacji w obszarze przyszłej wymiany mikrodanych w związku z planowaną certyfikacją w 2019 r. i zgodnie z wymaganiami Eurostatu.

## III. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa pt. **„Przeprowadzenie audytu bezpieczeństwa informacji dla systemu wymiany mikrodanych wg wymagań Wspólnych Ram Bezpieczeństwa Europejskiego Systemu Statystycznego”**.

Wymagania szczegółowe:

1. System informacyjny objęty audytem składa się z wydzielonego obszaru dla mikrodanych i obszaru dotyczącego całej organizacji zależnie od wymagań Wspólnych Ram Bezpieczeństwa IT ESS:
  - a. Obszar MDE (ang. *Micro Data Exchange*) będzie składał się z:
    - i. Projektowany obszar wymiany mikrodanych (Obszar wymiany)
    - ii. Obszar przetwarzania i składowania mikrodanych w istniejącej Operacyjnej Bazie Mikrodanych
  - b. Całość organizacji (przez organizację rozumie się jednostki organizacyjne statystyki publicznej, szczególnie Centrum Informatyki Statystycznej i Główny Urząd Statystyczny).
  - c. Docelowe środowisko wymiany i przetwarzania będzie gotowe na przełomie 2018 i 2019 r.
2. Docelowy proces przepływu danych:

- a. Odbieranie mikrodanych z Państw członkowskich:
    - i. Odbieranie przez bezpieczną sieć (obszar wymiany) z hubu Eurostatu za pomocą aktualnie testowanego komponentu dostarczanego przez Eurostat.
    - ii. Przetwarzanie i składowanie mikrodanych (obszar OBM).
  - b. Wysyłanie mikrodanych (dane krajowe):
    - i. Zależnie od możliwości MF przez bezpieczną sieć / bezpieczny szyfrowany nośnik przenoszony fizycznie z MF do GUS/CIS (obszar wymiany).
    - ii. Walidację danych z MF przed wysłaniem przy użyciu zautomatyzowanych skryptów (obszar wymiany).
    - iii. Przetwarzanie i składowanie mikrodanych (obszar OBM).
    - iv. Wysyłanie mikrodanych do hubu Eurostatu za pomocą obecnie testowanego komponentu Edamis4 dostarczanego przez Eurostat (obszar wymiany).
3. Dokumentacja bezpieczeństwa informacji w organizacji:
- a. Polityka Bezpieczeństwa Informacji Statystyki Publicznej (zasady ogólne, role i obowiązki, ogólna klasyfikacja informacji, dokument o charakterze organizacyjnym)
  - b. Dokumenty uzupełniające
  - c. Obszar OBM posiada wdrożoną dokumentację bezpieczeństwa.
  - d. Obszar wymiany posiada przygotowaną dokumentację bezpieczeństwa.
4. Zakres audytu został określony w tabeli nr 1.
- a. Tabela nr 1 zawiera listę wszystkich wymagań które powinny zostać poddane audytowi.
  - b. W tabeli nr 1 zakres wymagań audytowych został oznaczony słowem „TAK” odpowiednio dla każdego z obszarów. W przypadku wymagania obejmującego zakresem obszar MDE należy zaudytować wyłącznie ten wydzielony obszar.
  - c. Wymagane dowody spełnienia wymagań określone zostały szczegółowo w dokumencie „Wspólne ramy bezpieczeństwa IT ESS” (załącznik nr 1 do OPZ w języku angielskim, arkusz „Evidence”).
  - d. Audytu należy dokonać jedynie w zakresie wskazanym w OPZ z zastosowaniem dowodów wskazanych w dokumencie „Wspólne ramy bezpieczeństwa IT”.
5. Informacje uzupełniające:
- a. Infrastruktura bezpieczeństwa i informatyczna zlokalizowana jest w budynku GUS.
  - b. Pracownicy służb statystyki publicznej zaangażowani w proces wymiany i przetwarzania mikrodanych są wyłącznie pracownikami Głównego Urzędu Statystycznego i Centrum Informatyki Statystycznej pracującymi w budynku GUS.

6. Metodologia audytu powinna być zgodna z zaleceniami dla audytorów bezpieczeństwa rodziny norm ISO27000, w szczególności PN-ISO:IEC 27006:2016.
7. Z audytu należy sporządzić raport w języku polskim i angielskim (o tej samej treści i podobnym układzie). Raport w języku angielskim musi jako załącznik zawierać wypełniony arkusz „Audit”, kolumna K pt. „Answer”, z Załącznika nr 1 do OPZ, stanowiący procentowe określenie poziomu spełnienia poszczególnych wymagań.
8. Raporty muszą być zgodne z wymaganiami określonymi w pkt IV.
9. Spotkania robocze Zamawiającego z Wykonawcą będą odbywać się w siedzibie Zamawiającego.
10. Na potrzeby opracowania przedmiotu zamówienia Zamawiający udostępni w siedzibie Zamawiającego i po podpisaniu umowy posiadane materiały i dokumenty, jak również zapewni współpracę właściwych pracowników.

Tabela nr 1 – Lista wymagań bezpieczeństwa informacji i zakres przedmiotowy

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Information Security Policies	Polityki bezpieczeństwa informacji						
Policies for information security	Polityki dotyczące bezpieczeństwa informacji	Information Security policies have been defined	Polityki bezpieczeństwa informacji zostały określone	Organizacja	-	-	TAK
		Information Security policies have been approved by top organization management	Polityki bezpieczeństwa zostały zatwierdzone przez kierownictwo		-	-	TAK
		Policies have been internally published	Polityki bezpieczeństwa zostały opublikowane w organizacji		-	-	TAK
		Policies have been communicated to relevant parties, employees and external parties	Polityki zostały zakomunikowane pracownikom i właściwym stronom zewnętrznym		-	-	TAK
Review of the policies for information security	Przegląd polityk bezpieczeństwa informacji	Policies review is set within a specific interval (at least yearly) or when significant corporate changes related to information security occurs.	Polityki są poddawane przeglądom w zaplanowanych odstępach czasu (co najmniej raz w roku) lub wtedy kiedy wystąpią istotne zmiany w organizacji	Organizacja	-	-	TAK
		Review period is approved by management.	Przegląd okresowy jest zatwierdzany przez kierownictwo		-	-	TAK
		Adequacy of the information security policy is reviewed.	Przeglądowi poddana jest adekwatność polityk bezpieczeństwa		-	-	TAK

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
		Effectiveness of the information security policy is reviewed.	Przeglądowi poddana jest skuteczność polityk bezpieczeństwa		-	-	TAK
<b>Organisation of information security</b>	<b>Organizacja bezpieczeństwa informacji</b>						
Information security roles and responsibilities	Role i odpowiedzialność za bezpieczeństwo informacji	Information security roles and responsibilities have been defined into the organization	Role i odpowiedzialność za bezpieczeństwo informacji zostały określone w organizacji	Organizacja	-	-	TAK
Segregation of duties	Rozdzielenie obowiązków	Duties and areas of responsibility are separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services	Obowiązki i odpowiedzialność są rozdzielone w celu ograniczenia okazji do nieuprawnionej i nieumyślnej modyfikacji i nadużycia aktywów informacyjnych lub usług	Organizacja	-	-	TAK
		Assets are protected against unauthorized or unintentional modifications	Aktywa są chronione przed nieautoryzowaną lub nieumyślną modyfikacją				TAK
		Assets are prepared to minimize opportunities of misuse or abuse	Aktywa są utrzymywane w sposób minimalizujący okazje do błędnego użycia lub nadużycia				TAK
Information security in project management	Bezpieczeństwo informacji w zarządzaniu projektami	Information security assessment is included into project lifecycle management	Bezpieczeństwo informacji jest uwzględnione w procesie zarządzania projektami	MDE	TAK	TAK	-
<b>Humane resources security</b>	<b>Bezpieczeństwo zasobów ludzkich</b>						

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Terms and conditions of employment	Warunki zatrudnienia	Employees, contractors and third party users have signed confidentiality and non-disclosure agreements	Pracownicy, kontrahenci i strony zewnętrzne podpisują zobowiązanie do zachowania poufności i nieujawniania informacji	Organizacja	-	-	TAK
Management responsibilities	Odpowiedzialność kierownictwa	All levels managers are engaged in driving security within the business	Kierownictwo jest zaangażowane w proces zapewnienia bezpieczeństwa informacji	Organizacja	-	-	TAK
		Management behaviour encourages to all employees, contractors and 3rd party users to apply security in accordance with corporate policies and	Kierownictwo zachęca wszystkich pracowników, kontrahentów i strony zewnętrzne do przestrzegania wszelkich procedur i polityk w zakresie bezpieczeństwa informacji				TAK
Information security awareness, education and training	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Internal employees, contractors and 3rd party users receive regular information security updates	Pracownicy, kontrahenci i strony zewnętrzne regularnie otrzymują zaktualizowane polityki bezpieczeństwa	Organizacja	-	-	TAK
		Internal employees, contractors and 3rd party users are aware of information security policies and procedures and keep up-to-date with the latest changes	Pracownicy, kontrahenci i strony zewnętrzne mają świadomość obowiązków wynikających z polityk bezpieczeństwa i są zaznajomieni z ostatnimi zmianami				TAK
		Internal employees, contractors and 3rd party users undergo regular security awareness training appropriate to their role and function within the	Pracownicy, kontrahenci i strony zewnętrzne regularnie przechodzą szkolenia z zakresu bezpieczeństwa informacji odpowiednio do roli i funkcji w organizacji	MDE	TAK	TAK	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Asset management	Zarządzanie aktywami						
Inventory of assets	Inwentaryzacja aktywów	Assets are inventoried, associating each of them with information and information processing	Aktywa związane z informacjami i środkami przetwarzania informacji są zinwentaryzowane	MDE	TAK	TAK	-
		Asset inventory is accurated and kept up to date	Spis aktywów jest aktualizowany		TAK	TAK	-
Acceptable use of assets	Akceptowalne użycie aktywów	Acceptable use policy for each type of information asset is in place	Zasady (polityka) akceptowalnego użycia informacji są wdrożone dla każdego z rodzajów informacji	Organizacja	-	-	TAK
		Users are made aware about existance of this policy prior asset usage	Pracownicy oraz użytkownicy podmiotów zewnętrznych korzystający lub posiadający dostęp do aktywów organizacji zostali uświadomieni w kwestii wymagań bezpieczeństwa informacji		-	-	TAK
Return of assets	Zwrot aktywów	Process in place to ensure all employees return the organisation's assets on termination of their employment, contract or agreement	Wdrożono sformalizowany proces zakończenia stosunku pracy w taki sposób, aby obejmował zwrot wszystkich wydanych wcześniej fizycznych i elektronicznych aktywów należących do organizacji lub powierzonych organizacji.	MDE	TAK	TAK	-
Classification of information	Klasyfikacja informacji	Information classification scheme is defined and	Schemat klasyfikacji został zdefiniowany i jest wykorzystywany	Organizacja	-	-	TAK
		Information classified is according to the applicable legal requirements	Informacje są klasyfikowane na podstawie wymagań prawnych.		-	-	TAK



Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
		Information is classified according to the sensitivity of possible unauthorized disclosure or	Informacje są klasyfikowane z uwzględnieniem wrażliwości na nieuprawnione ujawnienie lub modyfikację.		-	-	TAK
		Information is classified according to how valuable it is to the organization (alignment with	Informacje są klasyfikowane na podstawie wartości dla organizacji.		-	-	TAK
Labelling of information	Znakowanie informacji	Information labeling procedures are accordingly to the information classification scheme	Procedury znakowania informacji są zgodne z przyjętym w organizacji schematem klasyfikacji informacji.	MDE	TAK	TAK	-
		There is a process or procedure for ensuring information classification is appropriately marked on each asset	Istnieje procedura zapewniająca znakowanie informacji odpowiednio dla każdego rodzaju aktywów.		TAK	TAK	-
Handling of assets	Postępowanie z aktywami	There is a procedure for handling each information classification	Istnieje procedura postępowania z aktywami dla każdego rodzaju aktywów	Organizacja	-	-	TAK
		Procedure for information handling is accordingly to information classification scheme	Procedura postępowania z aktywami jest zgodna ze schematem klasyfikacji informacji.	Organizacja	-	-	TAK
		Users of information assets are made aware about corporate procedure	Użytkownicy aktywów informacyjnych zostali uświadomieni o konieczności stosowania procedur.	Organizacja	-	-	TAK
Management of removable media	Zarządzanie nośnikami wymiennymi	There is a policy in place governing removable media	Istnieje wdrożona polityka zarządzania nośnikami wymiennymi	MDE	TAK	TAK	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
		There is a process covering how removable media is managed	Istnieje proces określający jak nośniki wymienne są zarządzane.		TAK	TAK	-
		Processes are aligned with the information classification scheme	Procesy są zgodne ze schematem klasyfikacji informacji.		TAK	TAK	-
Disposal of media	Wycofywanie nośników	There is a formal procedure in place governing how removable media no longer required is disposed	Istnieje procedura określająca bezpieczne wycofywanie nośników, które nie będą już dłużej wykorzystywane.		TAK	TAK	-
Physical media transfer	Przekazywanie nośników	There is a policy document and process detailing how physical media should be transported	Istnieje polityka i procedura określająca zasady transportu nośników fizycznych.		TAK	TAK	-
		Media in transport is protected against unauthorised access, misuse or corruption	Nośniki podczas transport są chronione przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności.		TAK	TAK	-
<b>Access control</b>	<b>Kontrola dostępu</b>						
Access control policy	Polityka kontroli dostępu	There is a documented access control policy in place	Istnieje wdrożona i udokumentowana polityka kontroli dostępu.	Organizacja	-	-	TAK
		Policy document is based on business	Polityka uwzględnia wymagania biznesowe.		-	-	TAK
		Policy is communicated appropriately	Polityka jest odpowiednio zakomunikowana użytkownikom		-	-	TAK

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Access to networks and network services	Dostęp do sieci i usług sieciowych	Controls are in place to ensure users only have access to the network resources they have been specially authorised to use and are	Zapewnienie użytkownikom dostępu wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.	MDE	TAK	TAK	-
User registration and de-registration	Rejestrowanie i wyrejestrowywanie użytkowników	There is a formal user access registration process in place	Istnieje formalny proces rejestrowania i wyrejestrowywania użytkowników.	Organizacja	-	-	TAK
User access provisioning	Przydzielanie dostępu użytkownikom	There is a formal user access provisioning process in place to assign or revoke access rights for all user types and devices	Istnieje wdrożony proces nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników	MDE	TAK	TAK	-
Management of privileged access rights	Zarządzanie prawami uprzywilejowanego dostępu	Privileged access accounts are separately managed and controlled	Prawa uprzywilejowanego dostępu są zarządzane oddzielnie i kontrolowane.	Organizacja	-	-	TAK
Management of secret authentication information of users	Zarządzanie poufnymi informacjami uwierzytelniającymi i użytkowników	There is a formal management process to control the allocation of secret authentication information established	Istnieje wdrożony proces zarządzania przydzielaniem poufnych informacji uwierzytelniających.	MDE	TAK	TAK	-
Review of user access rights	Przegląd praw dostępu użytkowników	There is a process for asset owners to review access rights to their assets on a regular basis	Właściciele aktywów przeglądają prawa dostępu użytkowników w regularnych odstępach czasu zgodnie z wdrożonym procesem.	MDE	TAK	TAK	-
		This review process is verified	Proces przeglądu praw dostępu powinien być możliwy do zweryfikowania.	Organizacja	-	-	TAK

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Removal or adjustment of access rights	Odbieranie lub dostosowywanie praw dostępu	There is a process to ensure that user access rights are removed on termination of employment or contract, or adjusted upon change of role	Istnieje proces zapewniający że po zakończeniu zatrudnienia, umowy lub porozumienia przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji są odbierane,	Organizacja	-	-	TAK
Use of secret authentication information	Stosowanie poufnych informacji uwierzytelniających	There is a policy document covering the corporate practices in how secret authentication information must be handled	Istnieje polityka zapewniająca że użytkownicy przestrzegają przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających.	Organizacja	-	-	TAK
		Policy document to manage secret information is communicated	Polityka została zakomunikowana wszystkim użytkownikom.		-	-	TAK
		It has been ensured that users understand how to handle with secret	Upewniono się, że użytkownicy wiedzą jak postępować z poufnymi informacjami.		-	-	TAK
Information access restriction	Ograniczanie dostępu do informacji	Access to information and application system functions is restricted in line with the access control	Istnieje ograniczanie dostępu do informacji oraz funkcji systemu aplikacyjnego zgodnie z polityką kontroli dostępu.	MDE	TAK	TAK	-
Secure log-on procedures	Procedury bezpiecznego logowania	Access is controlled by a secure log-on procedure where the access control policy requires it	Tam, gdzie polityka kontroli dostępu tego wymaga, zaleca się kontrolowanie dostępu do systemów i aplikacji przez procedurę bezpiecznego		TAK	TAK	-
Password management system	System zarządzania hasłami	There is a system to control password management	Ostał wdrożony system do kontroli zarządzaniami hasłami.		TAK	TAK	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
		Interactive password systems are in place	Interaktywny system zarządzania hasłami został wdrożony.		TAK	TAK	-
		Complex passwords following corporate	Zgodnie z polityką hasel wymaga się stosowania hasel dobrej jakości.		TAK	TAK	-
Use of privileged utility programs	Użycie uprzywilejowanych programów narzędziowych	Privilege utility programs are restricted and monitored	Użycie uprzywilejowanych programów narzędziowych jest ograniczone i monitorowane.		TAK	TAK	-
<b>Cryptography</b>	<b>Kryptografia</b>						
Policy on the use of cryptographic controls	Polityka stosowania zabezpieczeń kryptograficznych	There is a policy document in place on the use of cryptographic controls	Istnieje opracowana i wdrożona polityka stosowania zabezpieczeń kryptograficznych do ochrony informacji.	Organizacja	-	-	TAK
Key management	Zarządzanie kluczami	There is a policy governing the whole lifecycle of cryptographic keys	Istnieje polityka dotycząca korzystania, ochrony i okresów ważności kluczy kryptograficznych	Organizacja	-	-	TAK
<b>Physical and environmental security</b>	<b>Bezpieczeństwo fizyczne i środowiskowe</b>						
		There is a designated physical security perimeter	Określono fizyczne granice bezpieczeństwa.		TAK	TAK	-
Physical security perimeter	Fizyczna granica obszaru bezpiecznego	Areas which contains sensitive or critical information are appropriately	Obszary zawierające wrażliwe lub krytyczne informacje są odpowiednio kontrolowane.	MDE	TAK	TAK	-
		Areas which contains information processing facilities are segregated and appropriately	Obszary zawierające środki przetwarzania informacji są odpowiednio kontrolowane.		TAK	TAK	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Protecting against external and environmental threats	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Physical protection measures to prevent natural disasters, malicious attack or accidents have been designed	Zaprojektowanie i stosowanie fizycznych zabezpieczeń przed katastrofami naturalnymi, wrogim atakiem lub wypadkami.	MDE	TAK	TAK	-
Working in secure areas	Praca w obszarach bezpiecznych	There are secure areas in place	Zapewniono ustanowienie obszarów bezpiecznych.		TAK	TAK	-
		Secure areas have suitable policies and processes	Wdrożono procedury i polityki pracy w obszarach bezpiecznych.		TAK	TAK	-
		Policies and processes are enforced and monitored	Polityki procedury są wdrożone i monitorowane.		TAK	TAK	-
Equipment siting and protection	Lokalizacja i ochrona sprzętu	Environmental hazards are identified and considered when equipment locations are selected	Zaleca się umieszczenie i ochronę sprzętu w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych		TAK	TAK	-
		Risks from unauthorised access or passers-by are considered when siting equipment	Zaleca się umieszczenie i ochronę sprzętu w taki sposób, aby zredukować okazje do nieuprawnionego dostępu.		TAK	TAK	-
Cabling security	Bezpieczeństwo okablowania	Cabling security are located to protect from interference, interception or damage	Okablowanie jest chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem.	TAK	TAK	-	
Equipment maintenance	Konserwacja sprzętu	There is a procedure in place to ensure equipment availability	Istnieje procedura zapewniająca dostępność sprzętu.	TAK	TAK	-	
		There is a procedure in place to ensure equipment integrity	Istnieje procedura zapewniająca integralność sprzętu.	TAK	TAK	-	

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji	
		There is a rigorous equipment maintenance schedule	Istnieje plan konserwacji sprzętu.		TAK	TAK	-	
Secure disposal or reuse of equipment	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	There is a policy covering how information assets may be	Istnieje polityka ponownego wykorzystania zasobów	Organizacja	-	-	TAK	
		It is verified that all sensitive information and licensed software is properly removed before reuse/disposal where data is wiped	Przed zbyciem lub przekazaniem sprzętu do ponownego użycia zaleca się sprawdzenie wszystkich jego składników zawierających nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadnisane.		-	-	TAK	
Clear desk and clear screen policy	Polityka czystego biurka i ekranu.	A clear desk and clear screen policy is in place	Istnieje polityka czystego biurka i czystego ekranu.		-	-	-	TAK
		Clear desk and clear screen policy is well enforced	Prawidłowo wdrożono polityki czystego biurka i czystego ekranu.		-	-	-	TAK
<b>Operations security</b>	<b>Bezpieczna eksploatacja</b>							
Documented operating procedures	Dokumentowanie procedur eksploatacyjnych	Operating procedures are fully documented	Procedury eksploatacyjne są w pełni udokumentowane	MDE	TAK	TAK	-	
		Procedures are made available to all users when needed	Procedury eksploatacyjne są udostępniane wszystkim potrzebującym użytkownikom.		TAK	TAK	-	
Change management	Zarządzanie zmianą	Controlled change management process is in place for changes related to the security	Istnieje process zarządzania zmianą związaną z bezpieczeństwem informacji.	Organizacja	-	-	TAK	

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Capacity management	Zarządzanie pojemnością	There is in place a capacity management process	Istnieje proces zarządzania pojemnością.	MDE	TAK	TAK	-
Separation of development, testing and operational environments	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	A process to reduce the risk against unauthorized changes into operational environment	Wdrożono proces zmniejszający ryzyko nieautoryzowanych zmian w środowiskach produkcyjnych.		TAK	TAK	-
		Unauthorized accesses to operational environment is prevented	Zapobiega się nieautoryzowanemu dostępowi do środowisk produkcyjnych.		TAK	TAK	-
		The organisation enforces segregation of development, test and operational	Organizacja zapewnia oddzielenie środowisk rozwojowych, testowych i produkcyjnych.	MDE	TAK	TAK	-
Controls against malware	Zabezpieczenia przed szkodliwym oprogramowaniem	Processes to detect malware are in place	Istnieją procesy wykrywające szkodliwe oprogramowanie.	Organizacja	-	-	TAK
		Processes to prevent malware spreading have been developed and	Wdrożono procesy zapobiegające rozprzestrzenianiu się szkodliwego oprogramowania.		-	-	TAK
		Corporate process and capacity to recover from a malware infection is in place	Istnieje proces i zdolność organizacyjna do przywrócenia działania po infekcji szkodliwym oprogramowaniem.		-	-	TAK
		Appropriate malware awareness activity campaigns are carried out	Prowadzone są wewnętrzne kampanie dot. szkodliwego oprogramowania.		-	-	TAK
Information backup	Kopie zapasowe	A backup policy document has been implemented to cover business needs	Wdrożono politykę kopii zapasowych zgodną z wymaganiami biznesowymi.	MDE	TAK	TAK	-
		Backups are made in accordance	Kopie zapasowe wykonuje się zgodnie z polityką.		TAK	TAK	-



Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
		The organisation's backup policy complies with relevant legal frameworks	Polityka kopii zapasowych jest zgodna z odpowiednimi wymaganiami prawnymi.		TAK	TAK	-
Event logging	Rejestrowanie zdarzeń	A process to record user activities and events is developed, mainly for activities related to	Istnieje process polegający na zapisie działalności użytkowników i zdarzeń związanych z bezpieczeństwem informacji.	MDE	TAK	TAK	-
		Appropriate event logs are maintained	Logi są utrzymywane.		TAK	TAK	-
Protection of log information	Ochrona informacji w dziennikach zdarzeń	Logging facilities are protected against tampering and unauthorised access	Środki służące rejestrowaniu zdarzeń oraz informacji w dziennikach zdarzeń są chronione przed manipulacją i nieuprawnionym		TAK	TAK	-
Administrator and operator logs	Rejestrowanie działań administratorów i operatorów	System administrator and sysop logs are maintained and protected	Działania administratorów są utrzymywane i chronione.		TAK	TAK	-
Clock synchronisation	Synchronizacja zegarów	Clocks within the organisation systems or within security domain are synchronized and based on a single time source for all	Wszystkie zegary istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa są zsynchronizowane z jednym wzorcowym źródłem czasu.		Organizacja	-	-
Installation of software on operational systems	Instalacja oprogramowania w systemach produkcyjnych	A process to control the installation of software onto operational systems is in place	Wdrożono procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych.	MDE	TAK	TAK	-
Management of technical vulnerabilities	Zarządzanie podatnościami technicznymi	Organisation has access to updated and timely information on technical vulnerabilities	Organizacja ma dostęp do informacji o podatnościach technicznych wykorzystywanych systemów	MDE	TAK	TAK	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
		A process to assess risks and react to any new vulnerabilities as they are discovered has	Ustanowiono proces zarządzania podatnościami technicznymi.	Organizacja	-	-	TAK
Restrictions on software installation	Ograniczenia w instalowaniu oprogramowania	Processes are in place to restrict how users install software	Ustanowiono i wdrożono zasady instalowania oprogramowania przez użytkowników.	Organizacja	-	-	TAK
<b>Communication security</b>	<b>Bezpieczeństwo komunikacji</b>						
Network controls	Zabezpieczenia sieci	A network management process is in place to protect information in systems and applications	Istnieje proces zarządzania siecią w celu ochrony informacji w systemach i aplikacjach.	MDE	TAK	TAK	-
Information transfer policies and procedures	Polityki i procedury przesyłania informacji	Organisational policies govern how information is transferred	Wdrożo politykę przesyłania informacji.	Organizacja	-	-	TAK
		Procedures for how data should be transferred are made available to all	Procedury przesyłania informacji są dostępne dla wszystkich pracowników.	Organizacja	-	-	TAK
		Relevant technical controls are in place to prevent non-authorised forms of data	Zastosowano odpowiednie środki techniczne by zapobiec nieautoryzowanemu przesyłaniu informacji.	MDE	TAK	TAK	-
Agreements on information transfer	Porozumienia dotyczące przesyłania informacji	Contracts with external parties and agreements within the organisation detail the requirements for securing business information in	Porozumienia uwzględniają bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi.	MDE	TAK	TAK	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Electronic messaging	Wiadomości elektroniczne	Security policies cover the use of information transfer while using electronic messaging	Polityki przesyłania informacji odnoszą się także do wiadomości elektronicznych.	Organizacja	-	-	TAK
Confidentiality or nondisclosure agreements	Umowy o zachowaniu poufności lub nieujawnianiu informacji	Employees, contractors and agents sign confidentiality or non disclosure agreements	Pracownicy, kontrahenci i strony zewnętrzne podpisują zobowiązanie do zachowania poufności i	Organizacja	-	-	TAK
		Records of the agreements are maintained	Utrzymywany jest rejestr umów.				TAK
<b>System acquisition, development and maintenance</b>	<b>Pozyskiwanie, rozwój i utrzymanie systemów</b>						
Information security requirements analysis and specification	Analiza i specyfikacja wymagań związanych z bezpieczeństwem informacji	Information security requirements are specified when new systems are introduced	Wymagania dotyczące bezpieczeństwa informacji są włączone do wymagań stawianych nowym systemom informacyjnym.	Nie dotyczy	-	-	-
		When systems are being enhanced or upgraded, security requirements are specified and addressed	Wymagania dotyczące bezpieczeństwa informacji są włączone do wymagań stawianych rozbudowywanym systemom.	MDE	TAK	TAK	-
Securing application services on public networks	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	Applications which send information over public networks appropriately protect the information against fraudulent activity, contract dispute, unauthorised	Aplikacje wysyłające informacje przesyłane w sieciach publicznych są chronione przez nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnionym ujawnieniem i	Nie dotyczy	-	-	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Protecting application services transactions	Ochrona transakcji usług aplikacyjnych	Controls are in place in order to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay attacks	Istnieją zabezpieczenia informacji, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu powieleniu lub odtworzeniu.	MDE	TAK	TAK	-
Secure development policy	Polityka bezpieczeństwa prac rozwojowych	Organisation develops software or systems	Organizacja zapewnia rozwój oprogramowania i systemów	MDE	TAK	TAK	-
		Policies are mandating the implementation and assessment of security controls for development	Polityka określa zasady wdrożenia i oceny zabezpieczeń dla prac rozwojowych.		TAK	TAK	-
Restrictions on changes to software packages	Ograniczenia dotyczące zmian w pakietach oprogramowania	A policy is in place which mandates when and how software packages can be changed or	Istnieje polityka określająca kiedy i w jaki sposób można modyfikować pakiety oprogramowania		TAK	TAK	-
Outsourced development	Prace rozwojowe zlecane podmiotom zewnętrznym	Development is supervised when it has been outsourced	Organizacja nadzoruje prace rozwojowe nad systemami zleczone podmiotom zewnętrznym.		TAK	TAK	-
		Externally developed code is subject to a security review before deployment	Kod źródłowy opracowany przez podmiot zewnętrzny powinien być sprawdzony przed wdrożeniem.	TAK	TAK	-	
<b>Supplier relationships</b>	<b>Relacje z dostawcami</b>						

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Information security policy for supplier relationships	Bezpieczeństwo informacji w relacjach z dostawcami	Information security is included in contracts established with suppliers and service providers to mitigate possible risks	Uzgodnienie z dostawcą i udokumentowanie wymagań bezpieczeństwem informacji celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji.	MDE	TAK	TAK	-
		It is an organisation-wide risk management approach to supplier	W relacjach z dostawcami organizacja stosuje podejście oparte na zarządzaniu ryzykiem.	Organizacja	-	-	TAK
<b>Information security incident</b>	<b>Zarządzanie incydentami związanymi z bezpieczeństwem informacji</b>						
Responsibilities and procedures	Odpowiedzialność i procedury	A procedure to establish the information security incident	Istnieje procedura reagowania na incydenty bezpieczeństwa	Organizacja	-	-	TAK
		Management responsibilities are clearly identified and documented in the incident management	W procesie zarządzania incydentami określono odpowiedzialność kierownictwa.	Organizacja	-	-	TAK
Reporting information security events	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Information security events are reported by all employees and contractors using the appropriate management	Zdarzenia są zgłaszane przez odpowiedni kanał komunikacji przez wszystkich pracowników i kontrahentów.	MDE	TAK	TAK	-
Reporting information security weaknesses	Zgłaszanie słabości związanych z bezpieczeństwem informacji	A process for employees and contractors has been developed in order to report identified information security weaknesses	Słabości związane z bezpieczeństwem informacji są zgłaszane zgodnie z procedurą przez wszystkich pracowników i kontrahentów.	Organizacja	-	-	TAK
Assessment of and decision on information security events	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem	Corporate process has been done to ensure that information security events	Wdrożono proces zapewniający że zdarzenia są oceniane właściwie.	Organizacja	-	-	TAK

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Response to information security incidents	Reagowanie na incydenty związane z bezpieczeństwem informacji	It has been set-up an incident response process which reflects the classification and severity of information	Wdrożono process reagowania na incydenty z klasyfikacją incydentów.	Organizacja	-	-	TAK
Learning from information security incidents	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	A process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events is in place	Istnieje proces w wykorzystujący wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych	Organizacja	-	-	TAK
Collection of evidence	Gromadzenie materiału dowodowego	Forensic readiness policy has been created and established	Ustanowiono politykę gromadzenia materiału dowodowego.	Organizacja	-	-	TAK
		In the event of an information security incident a procedure where relevant data is identified and collected in a manner which allows it to be used as	Procedurya identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy.	MDE	TAK	TAK	-
<b>Information security aspects of business continuity management</b>	<b>Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania</b>						
Planning information security continuity	Planowanie ciągłości bezpieczeństwa informacji	Information security is included in the organisation's continuity plan and disaster recovery plan	Bezpieczeństwo informacji jest włączone w plan ciągłości działania i plan odtworzenia po katastrofie.	MDE	TAK	TAK	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Implementing information security continuity	Wdrożenie ciągłości bezpieczeństwa informacji	Organisation information security function has documented, implemented and maintained policies, processes and procedures to maintain continuity of service during	Ustanowiono, udokumentowano, wdrożono i utrzymuje się procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji		TAK	TAK	-
<b>Compliance</b>	<b>Zgodność</b>						
Identification of applicable legislation and contractual requirements	Określenie stosownych wymagań prawnych i umownych	Organisation has identified and documented all relevant legislative, regulatory or contractual requirements related to	Dla każdego systemu informacyjnego oraz całości organizacji zidentyfikowano, udokumentowano i zaktualizowano istotne wymagania prawne,	Organizacja	-	-	TAK
Protection of records	Ochrona zapisów	Records are protected from loss, destruction, falsification and unauthorised access or release in accordance with legislative, regulatory, contractual and business	Zapisy są chronione przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem stosownie do wymagań prawnych, administracyjnych, umownych i	Organizacja	-	-	TAK
Privacy and protection of personally identifiable information	Prywatność i ochrona danych identyfikujących osobę	Policy for privacy and protection of personally identifiable information has been developed	Opracowano i wdrożono politykę dotyczącą prywatności i ochrony danych identyfikujących osobę.	MDE	TAK	TAK	-
		Personal data is protected in accordance with relevant legislation	Dane osobowe są chronione zgodnie z właściwymi wymaganiami prawnymi.		TAK	TAK	-

Nazwa rozdziału (angielska)	Nazwa rozdziału (polska)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. angielski)	Wymaganie z dokumentu „Wspólne ramy bezpieczeństwa IT ESS” (jęz. polski)	Zakres	Obszar wymiany	Obszar OBM	Obszar organizacji
Regulation of cryptographic controls	Regulacje dotyczące zabezpieczeń kryptograficznych	Cryptographic controls are protected in accordance with all relevant agreements, legislation and regulations	Zabezpieczenia kryptograficzne są stosowane zgodnie z odpowiednimi umowami, wymaganiami prawnymi i administracyjnymi.	Organizacja			TAK



#### **IV. Wymagania dla dokumentów**

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.

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 i angielskim, 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., wynikająca z księgi znaków Zamawiającego, zostanie przekazana Wykonawcy po podpisaniu umowy.
3. 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.
4. 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.

#### **V. 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, 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 umowy.