Załącznik nr …… do Umowy ……

Szczegółowe wymagania dotyczące dokumentacji systemu informatycznego

I. Cel dokumentu

Dokument zawiera szczegółowe wymagania dotyczące formy oraz zawartości dokumentacji dostarczanej przez Wykonawcę wraz z systemem informatycznym.

II . Zakres wymagań dotyczący dokumentacji

1. Uwagi i wymagania ogólne

1. Dokumentacja powinna zostać dostarczona w wersji elektronicznej edytowalnej i dodatkowo w wersji papierowej. W związku z powyższym wersja elektroniczna powinna być dostarczona dla:
   a) dokumentów tekstowych w formacie PDF z możliwością przeszukiwania, również wyrazów z polskimi znakami i możliwością zaznaczania kopiowania treści,
   b) dokumentów tekstowych w formacie DOC (lub innym ogólnie dostępnym formacie edytowalnym).
2. W przypadku diagramów, schematów dostarczonych w ramach dokumentacji powinny one być dostarczone w narzędziu zgodnym z notacjami UML, BPMN, Archimate i zapisane w formacie umożliwiającym ich przeglądanie w dostępnych publicznie i darmowych narzędziach, wraz ze wskazaniem źródła ich pobrania lub poprzez dostarczenie niezbędnego do przeglądania oprogramowania w ramach projektu.
3. Dokumentacja powinna uwzględniać zarówno środowisko produkcyjne, testowe/szkoleniowe, jak i deweloperskie systemu.
4. Zawartość dokumentacji powinna być czytelna (dotyczy grafik, wykresów, diagramów).
5. Zalecenia Zamawiającego w odniesieniu do wymagań edytorskich:
   a) szablon dokumentu z wymaganymi elementami zgodny z standardem obowiązującym u Zamawiającego (zostanie przekazany Wykonawcy),
   b) preferowany format dokumentacji (wielkość strony) –A4,
   c) czcionka o kroju Verdana,
   d) wersjonowanie dokumentacji – format wersji n.xx gdzie n oznacza numer kolejnej zatwierdzonej wersji dokumentu, xx – numer kolejnej wersji opiniowanej, roboczej.

2. Opis systemu

Opis techniczny systemu powinien obejmować:

1. Schemat blokowy systemu wraz z opisem jego składowych oraz przepływu i przetwarzania danych w systemie.
2. Diagram wdrożenia (deployment diagram) obejmujący wszystkie składowe systemu (w nomenklaturze UML: węzły, środowiska wykonawcze, komponenty/artefakty), wraz ze ścieżkami komunikacji pomiędzy składowymi oraz systemami zewnętrznymi z opisem wykorzystywanych protokołów i portów wszystkich uruchomionych w systemie usług.

3. Dokumentacja administratora

3.1. Opis zarządzania użytkownikami i uprawnieniami w systemie w warstwie aplikacyjnej

Zapisy dotyczące zarządzania użytkownikami i uprawnieniami w warstwie aplikacyjnej powinny zawierać opis zawierający:

1. Proces tworzenia i usuwania użytkowników oraz modyfikacji i odbierania uprawnień (w formie instrukcji) w warstwie oprogramowania funkcjonalnego systemu.
2. Wykaz ról, profili użytkownika i przywilejów zdefiniowanych w systemie wraz z opisem.
3. Raportowanie uprawnień użytkowników.
4. Opis dotyczący implementacji audytu historii aktywności użytkownika.

3.2. Opis konfiguracji stacji roboczej lub urządzenia klienckiego dla użytkownika systemu

Opis powinien zawierać proces przygotowania i konfiguracji stacji roboczej lub urządzenia klienckiego dla użytkownika pracującego w systemie.

Opis przygotowania i konfiguracji stacji roboczej przeznaczonej do pracy w systemie powinien zawierać:

1. Listę oprogramowania, zawierającą nazwę oprogramowania, producenta, wersję, źródło pakietów instalacyjnych.
2. Wymagania sprzętowe.

3. Wymagania dotyczące systemu operacyjnego oraz dodatkowego oprogramowania ze wskazaniem wersji minimalnej.
4. Instrukcję instalacji oprogramowania.

3.3. Opis wymagań dla systemów teleinformatycznych w odniesieniu do rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)

Opis powinien uwzględniać wymagania zawarte w Rozporządzeniu Rady Ministrów z dn. 16.05.2016 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dokumentacja systemu teleinformatycznego powinna zawierać m.in.:

1. Opis kodowania znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków.
2. Opis formatów danych w jakim udostępniane są zasoby informacyjne zgodnie z załącznikiem nr 2 do rozporządzenia.
3. Opis logów, dzienników systemów zawierających odnotowanie działań użytkowników lub obiektów systemowych polegające na dostępie do:
   a) systemu z uprawnieniami administracyjnymi;
   b) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
   c) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
4. Opis logów, dzienników systemów zawierający działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:
   a) działań użytkowników nieposiadających uprawnień administracyjnych,
   b) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
   c) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny.

4. Licencje i gwarancje

4.1. Licencje

W dokumentacji, wykonawca zobowiązany jest przedstawić listę wszystkich licencji na dostarczone oprogramowanie wraz z opisem sposobu licencjonowania. Opis powinien dotyczyć wszystkich aplikacji wymagających licencjonowania (aplikacje, systemy operacyjne, bazy danych, urządzenia i inne).

Lista licencji na oprogramowanie powinna zawierać:

1. Nazwę oprogramowania.
2. Sposób licencjonowania (np. procesor, użytkownik; informacje o metryce, uprawnieniach, ograniczeniach).
3. Ilości, rodzaje licencji (np. enterprise, standard) oraz poziom licencji.
4. Numer licencji.

5. Procedury

5.1. Procedury eksploatacyjne

Procedury mające na celu zabezpieczenie, bieżące utrzymanie i zapewnienie wysokiej niezawodności działania systemu.

1. Przekazanie inicjalnych haseł do kont administracyjnych systemu wraz z procedurą bezpiecznej zmiany haseł (bez wpływu na funkcjonowanie systemu).

6. Dokumentacja użytkownika

W przypadku dokumentacji eksploatacyjnej, w której przewidziane są różne kategorie użytkowników, należy uwzględnić instrukcje dla wszystkich grup użytkowników. Minimalna zawartość dokumentacji dla użytkownika powinna obejmować:

1. Instrukcję rozpoczęcia, zawieszania i zakończenia pracy w systemie.
2. Instrukcję użytkownika zawierającą opis wykonywania zadań w systemie z uwzględnieniem różnych wariantów ich wykonania.
3. Szczegółowy opis funkcjonalności systemu.
4. Opis ścieżek obsługi procesów.
5. Dokładny opis raportów generowanych w systemie. Opis powinien zawierać informacje dotyczące parametryzacji, filtrowania i innych

elementów personalizacyjnych dostępnych dla użytkownika oraz proces eksportowania raportów do narzędzi zewnętrznych.

6. Opis komunikatów błędu wraz z podaniem rozwiązań.
7. Przedstawienie systemu pomocy.
8. Instrukcja pracy awaryjnej.
9. Szkolenie w wersji elektronicznej, w formie pozwalającej na przeprowadzenie szkolenia w oprogramowaniu (Moodle), wraz z prawem licencyjnym pozwalającym w szczególności na:
   a) swobodne wykorzystanie przekazanych materiałów w ramach kursu na potrzeby szkoleniowe, w zakresie w jakim CUI uzna za stosowne,
   b) swobodną ingerencję dotyczącą zawartości kursu w tym zawartości merytorycznych jak i treści, materiałów graficznych i audiowizualnych zawartych w przekazanym kursie.

7. Wymogi dokumentacji w odniesieniu do danych osobowych

Informacje dotyczące przetwarzanych danych osobowych powinny zostać zebrane w osobnym dokumencie poświęconemu temu zagadnieniu.

Dokument powinien zawierać elementy odnoszące się do przetwarzania, w tym przechowywania danych osobowych (tzw. zwykłych bądź szczególnych kategorii) w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub RODO) oraz ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.

W przypadku przetwarzania w systemie danych osobowych wymagane jest opisanie następujących elementów:

1. Wykaz lokalizacji tworzących obszar w których przetwarzane są dane osobowe (wykaz budynków, pomieszczeń lokalizacji serwerów i stacji roboczych).
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
3. Opis struktury zbiorów danych wraz ze schematem wskazującym zawartość poszczególnych pól informacyjnych i powiązania między nimi. Minimalny zakres powinien zawierać:

- schemat bazy danych,
- nazwy tabel,
- nazwy pól,
- właściwości pól,
- opisane klucze główne i/lub obce.

4. Logiczną interpretacją danych jak również sposób przepływu danych pomiędzy poszczególnymi systemami/podsystemami na poziomie szczegółowości określonej w podpunkcie 2.
5. Opis dostarczonych rozwiązań technicznych oraz organizacyjnych zapewniających realizację praw podmiotu danych opisanych w art.12-18 i 20-22 RODO w tym poufność, integralność i rozliczalność przetwarzanych danych z uwzględnieniem:
    a)Opisu zawierającego implementację realizacji przez system automatycznego zapisywania zatwierdzonych w systemie danych wraz z wskazaniem miejsca przechowywania informacji w systemie (na poziomie szczegółowości określonym w podpunkcie 2):
    - realizacja zasady rozliczalności w systemach informatycznych,
        - daty pierwszego wprowadzenia danych do systemu oraz kolejnych dat ich modyfikacji,
        - identyfikatora użytkownika wprowadzającego oraz modyfikującego dane,
        - informacji audytowych zawierających historię poszczególnych wartości zmodyfikowanych z jednoznacznym przypisaniem ich do identyfikatora użytkownika przeprowadzającego modyfikacje w systemie,
    - informacji o odbiorcach, w rozumieniu art. 4pkt 9)RODO, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,
    - funkcjonalności systemu służące do wersjonowania rożnych treści zgód, treści klauzul informacyjnych, regulaminów itp.,
    - dokumentowanie źródła pozyskania danych w systemie.
    - możliwości realizacji prawa ograniczenia przetwarzania (prawa do sprzeciwu),
    - możliwości realizacji prawa do bycia zapomnianym,

- możliwość realizacji prawa do otrzymania kopii danych w maszynowym formacie,
- wbudowania w system funkcjonalności obejmujących szyfrowanie, anonimizację danych, pseudonimizację danych, zabezpieczenia dotyczące pseudonimizacji,
- funkcjonalności „archiwum", sposób realizacji w systemach informatycznych zakończenia przetwarzania w podstawowym celu, (okresy retencji),

b) Opisu zawierającego mechanizm logowania do systemu i przechowywania historii logowań do systemu zawierający wskazanie miejsca przechowywania informacji dotyczących:

- Datę prób logowań do systemu z informacją o udanym lub nie procesie logowania przez użytkownika,
- Identyfikator użytkownika,
- Adres IP urządzenia z którego nastąpiło zalogowanie/próba logowania.

c) Wykaz uprawnień – ról, profili dających dostęp do danych osobowym lub wrażliwych z wyszczególnieniem praw dostępowych do danych (odczyt, zapis, modyfikacja).

d) Zapis potwierdzający implementację w systemie automatycznego mechanizmu wymuszającego zmianę hasła przez użytkownika co 30 dni.

e) Opis zawierający dostęp do funkcjonalności umożliwiającej sporządzenie raportu i jego wydruk w zakresie informacji wskazanych w podpunktach a, b oraz c (w przypadku podpunktu c raport umożliwiający wygenerowanie raportu na poziomie poszczególnych użytkowników).

6. Opis zastosowanych metod i środków uwierzytelniania.

7. Opis elementów programowych i sprzętowych zabezpieczający system informatyczny przed działaniem szkodliwego oprogramowania oraz oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu.

8. Opis zabezpieczeń chroniących przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

9. Opis zawierający wyszczególnienie realizacji pozostałych wymogów odnoszących się do środków technicznych i organizacyjnych dla poziomu bezpieczeństwa zdefiniowanym na poziomie wysokim Załącznik 5 niniejszego dokumentu.
10. Dokument powinien zawierać odwołania do instrukcji użytkownika oraz procedur eksploatacyjnych zwierających informacje o:
    a) Procedurze i instrukcji rozpoczęcia, zawieszania i zamykania pracy w systemie
    b) Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.
    c) Sposobie, miejscu i okresie przechowywania nośników informacji zawierających dane osobowe oraz kopie zapasowe określone w podpunkcie b).
    d) Procedurze wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

8 Wymagania dodatkowe dla dokumentacji dotyczącej usług w architekturze chmury obliczeniowej

W przypadku rozwiązań opartych na modelu przetwarzania w chmurze obliczeniowej gdzie przetwarzane są dane osobowe, dostarczona dokumentacja powinna zawierać między innymi:

1. Informację o lokalizacjach serwerów na których przetwarzane są lub mogą być przetwarzane dane, z uwzględnieniem CPD głównych i zapasowych.
2. Wskazanie sposobu oraz zasad dostępu do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych przyjmowanych w poszczególnych centrach przetwarzania danych.
3. Listę zawierającą podwykonawców i współpracujących instytucji mających udział w realizacji usługi chmurowej wraz ze wskazaniem roli każdego z tych podmiotów w procesie przetwarzania danych osobowych.
4. Procedurę raportowania incydentów bezpieczeństwa w zakresie powierzonych danych.

IV. Załączniki

Załącznik 1. Lista kontrolna wymagań zakresu dokumentacji.

L.p	Rozdział	Podrozdział	Punkt	Wymagany zakres dokumentacji [T/N]	UWAGI
1	Uwagi i wymagania ogólne	-	1		
			2		
			3		
			4		
			5		
			6		
2	Opis systemu	-	1		
			2		
			3		
3	Infrastruktura przetwarzania i przechowywania danych	-	1		
			2		
			3		
			4		
			5		
			6		
			7		
4	System łączności	-	1		

			2		
			3		
			4		
			5		
			6		
			7		
			8		
			9		
			10		
5	Dokumentacja administratora	5.1. Opis konfiguracji systemu oraz wszystkich parametrów systemu w warstwie aplikacyjnej	1		
			2		
			3		
			4		
			5		
			6		
		5.2 Opis zarządzania użytkownikami i uprawnieniami w systemie w warstwie aplikacyjnej	1		
			2		
			3		
			4		
		5.3. Opis słowników wykorzystywanych w systemie	1		
			2		
			3		
		5.4. Opis konfiguracji stacji roboczej lub urządzenia klienckiego dla użytkownika systemu	1		
			2		
			3		
			4		
		5.5. Opis wymagań dla systemów teleinformatycznych w odniesieniu do rozporządzenia w sprawie KRI	1		
			2		
			3		
			4		
			5		
6	Licencje i gwarancje	6.1.Licencje	1		
			2		
			3		
			4		
		6.2.Gwarancje i serwis	1		
			2		
			3		
7	Procedury	7.1.Procedury eksploatacyjne	1		
			2		
			3		

			4		
			5		
		7.2 Procedury awaryjne i odtworzeniowe	1		
			2		
			3		
			4		
		7.3. Procedura wykonania kopii danych i konfiguracji z systemu produkcyjnego na testowy	1		
			2		
			3		
			4		
8	Dokumentacja użytkownika	-	1		
			2		
			3		
			4		
			5		
			6		
			7		
			8		
			9		
9	Wymogi dokumentacji w odniesieniu do danych osobowych	-	1		
			2		
			3		
			4		
			5		
			6		
			7		
			8		
			9		
			10		
		1.1. Wymagania dodatkowe dla dokumentacji dotyczącej usług w architekturze chmury obliczeniowej	1		
			2		
			3		
			4		
10	Wymagania dotyczące dokumentacji dla systemów w których prowadzone są księgi rachunkowe		1		
			2		
			3		

11	Wymagania dotyczące kodów źródłowych		1		
			2		
			3		

Załącznik 2. Zestawienie uzgodnień i protokołów podpisanych na etapie realizacji

Lp.	**Opis zakresu protokołu/uzgodnienia**	**Data zatwierdzenia**	**Uwagi**
…			

Załącznik 3. Globalny rejestr zmian w dokumentacji powykonawczej

Lp.	**Data zatwierdzania zmiany**	**Nazwa dokumentu**	**Numer wersji**	**Opis i zakres zmian**
…				

Załącznik 4.

Nie dotyczy

Załącznik 5. Wyciąg dotyczący minimalnych oraz dodatkowych środków technicznych i organizacyjnych które muszą być spełnione dla osiągnięcia poszczególnych poziomów bezpieczeństwa systemów informatycznych.

System powinien zapewniać poziom bezpieczeństwa: **Wysoki**.

W celu osiągnięcia poziomu wysokiego, niezbędne jest zapewnienie środków określonych dla poziomów bezpieczeństwa poziomu podstawowego, podwyższonego i wysokiego (tabela 1, 2 i 3)

Tabela 1. Poziom podstawowy

Lp.	Opis wymaganych rozwiązań technicznych lub organizacyjnych
I	*1. Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.* *2. Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.*
II	*1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.* *2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:* *a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;* *b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.*
III	*System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:* *1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;* *2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.*
IV	*1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.* *2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni. Hasło składa się co najmniej z 6 znaków.* *3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów oraz programów służących do przetwarzania danych.*
	4. Kopie zapasowe: *a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;* *b) usuwa się niezwłocznie po ustaniu ich użyteczności.*
V	*Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.*
VI	*Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:* *1) likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;* *2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;* *3) naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.*
VII	*Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego*

Tabela 2. Poziom podwyższony

Lp.	Opis wymaganych rozwiązań technicznych lub organizacyjnych
VIII	*1. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.*
IX	*Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.*
X	*Instrukcję zarządzania systemem informatycznym, o której mowa w § 5 Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika do Rozporządzenia.*

Tabela 3. Poziom wysoki

Lp.	Opis wymaganych rozwiązań technicznych lub organizacyjnych
XI	*1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.* *2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:* *a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;* *b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.*
XII	*Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej*