**Załącznik nr 23**
do Umowy nr.....
z dnia.....

# MINISTERSTWO FINANSÓW
# DEPARTAMENT INFORMATYKI

# DOKUMENTACJA BEZPIECZEŃSTWA

## <NAZWA SYSTEMU/USŁUGI>

**styczeń 2010**

| **MINISTERSTWO FINANSÓW<br>DEPARTAMENT INFORMATYKI** | | | | | | |
|---|---|---|---|---|---|---|
| **Dokument** | **DOKUMENTACJA BEZPIECZEŃSTWA <NAZWA SYSTEMU/USŁUGI>** | | | | | |
| **Krótki opis dokumentu** | | | | | | |
| **Opracowano na podstawie** | | | | | | |
| **Właściciel dokumentu** | Departament Informatyki | | | | | |
| **Weryfikacja merytoryczna** | Imię i nazwisko, stanowisko | | Data | | Podpis | |
| **Weryfikacja formalna** | Imię i nazwisko, stanowisko | | Data | | Podpis | |
| **Data druku** | | | | Liczba stron | | 13 |
| **Nazwa pliku** | | | | Status | | |

(*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja
(**) Rozdziały: numery rozdziałów lub W-Wszystkie

***{Informacje wstępne:***

*Niniejszy dokument jest wzorem do opracowania właściwej dokumentacji bezpieczeństwa dla danego systemu/usługi, obowiązującym w Ministerstwie Finansów oraz w jednostkach organizacyjnych resortu finansów.*
*Dokumentacja bezpieczeństwa dla danego systemu/usługi musi być opracowany według niniejszego układu, z uwzględnieniem właściwych dla danego systemu/usługi elementów.*
*W metryce dokumentu należy umieścić faktyczne dane dotyczące autorów, wersji i daty opracowania dokumentacji bezpieczeństwa systemu/usługi.*
*Tekstem pisanym kursywą, umieszczonym w nawiasach klamrowych, oznaczono komentarze dla autorów dokumentacji bezpieczeństwa tworzonych na podstawie niniejszego wzorca. W wersji finalnej komentarze te należy usunąć.*
*Pole oznaczone <nazwa systemu/usługi> należy w finalnej wersji dokumentu należy zastąpić właściwą nazwę systemu/usługi.}*

## SPIS TREŚCI


**WYKAZ SKRÓTÓW I TERMINÓW ..... 5**

**1. CEL DOKUMENTU ..... 5**

**2. ODPOWIEDZIALNOŚĆ ..... 5**

**3. ZAKRES I WARUNKI STOSOWANIA DOKUMENTU ..... 5**

**4. POWIĄZANIA Z INNYMI DOKUMENTAMI ..... 5**

*4.1. DOKUMENTY USTAWOWE ..... 5*
*4.2. DOKUMENTY NORMATYWNE MINISTERSTWA FINANSÓW ..... 5*
*4.3. NORMY I STANDARDY ..... 5*
*4.4. DOKUMENTACJA SYSTEMU I INNE DOKUMENTY PROJEKTOWE ..... 6*
*4.4.1. Dokumentacja systemowa ..... 6*
*4.4.2. Dokumentacja eksploatacyjna ..... 6*
*4.4.3. Dokumentacja administracyjna ..... 6*
*4.4.4. Dokumenty inne ..... 6*

**5. DEFINICJA SYSTEMU ..... 6**

*5.1. NAZWA SYSTEMU ..... 6*
*5.2. PRZEZNACZENIE SYSTEMU ..... 6*
*5.3. LOKALIZACJA SYSTEMU ..... 6*
*5.4. MIEJSCE SYSTEMU W INFRASTRUKTURZE INFORMATYCZNEJ RESORTU FINANSÓW ..... 6*
*5.5. PODMIOTY ODPOWIEDZIALNE ZA SYSTEM ORAZ JEGO EKSPLOATACJĘ ..... 6*
*5.6. ODBIORCY SYSTEMU ..... 7*

**6. OPIS SYSTEMU ..... 7**

*6.1. CHARAKTERYSTYKA I KLASYFIKACJA INFORMACJI W SYSTEMIE ..... 7*
*6.2. ARCHITEKTURA LOGICZNA SYSTEMU ..... 7*
*6.2.1. Warstwa interfejsu użytkownika ..... 7*
*6.2.2. Warstwa kontroli dostępu ..... 7*
*6.2.3. Warstwa aplikacji ..... 7*
*6.2.4. Warstwa bazy danych ..... 7*
*6.2.5. Inne warstwy ..... 7*
*6.3. PRZEPŁYW DANYCH I INFORMACJI W SYSTEMIE ..... 7*
*6.4. ARCHITEKTURA FIZYCZNA SYSTEMU ..... 7*
*6.4.1. Infrastruktura serwerowa z podziałem na realizowane funkcje ..... 7*
*6.4.2. Inne komponenty sprzętowe ..... 7*
*6.4.3. Połączenia i zależności pomiędzy poszczególnymi elementami ..... 7*
*6.4.4. Połączenia sieciowe ..... 7*
*6.4.5. Architektura środowiska sieciowego WAN/LAN ..... 7*
*6.4.6. System tworzenia kopiowania zabezpieczającego ..... 7*
*6.4.7. System monitorowania pracy systemu ..... 7*
*6.4.8. Wykorzystywane oprogramowanie systemowe i narzędziowe wraz z jego umiejscowieniem ..... 7*
*6.4.9. Wykorzystywane oprogramowanie użytkowe wraz z jego umiejscowieniem ..... 7*
*6.4.10. Wymagania sprzętowo-systemowe dla użytkownika końcowego ..... 7*
*6.5. PODZIAŁ RÓL W SYSTEMIE (REALIZACJI USŁUGI) ..... 8*
*6.6. ZABEZPIECZENIA KRYPTOGRAFICZNE ..... 9*
*6.6.1. Polityka wykorzystania zabezpieczeń kryptograficznych ..... 9*
*6.6.2. Rodzaje wykorzystywanych certyfikatów ..... 9*
*6.6.3. Zasady zarządzanie kluczami ..... 9*

**7. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE ..... 9**

*7.1. ..... **Błąd! Nie zdefiniowano zakładki.***
*7.2. MINIMALNE WYMAGANIA W ZAKRESIE OCHRONY STACJI ROBOCZYCH UŻYTKOWNIKÓW WEWNĘTRZNYCH ORAZ ZEWNĘTRZNYCH. ..... **Błąd! Nie zdefiniowano zakładki.***

*7.3. ELEMENTY ELEKTRONICZNEGO ŚRODOWISKA BEZPIECZEŃSTWA ... 9*
*7.6.1. Interfejsy człowiek-sprzęt wykorzystywane w systemie ... 9*
*7.6.2. Interfejsy pomiędzy elementami systemu o różnych klasach bezpieczeństwa ... 9*
*7.6.3. Interfejsy do innych systemów ... 9*
*7.6.4. Zasady podłączenia do zewnętrznych sieci łączności ... 9*
*7.6.5. Inne elementy elektronicznego środowiska bezpieczeństwa ... 9*

**8. ŚRODKI OCHRONY ZASOBÓW INFORMACYJNYCH SYSTEMU ... 10**

*8.1. ORGANIZACYJNE I PRAWNE ŚRODKI OCHRONY ... 10*
*8.2. INFORMATYCZNE ŚRODKI OCHRONY ... 10*
*8.2.1. Środki ochrony przed awarią systemu ... 10*
*8.2.2. Środki ochrony konfiguracji systemu ... 10*
*8.2.3. Środki ochrony dostępu do systemu ... 10*
*8.2.4. Środki ochrony integralności danych ... 10*
*8.2.5. Inne informatyczne środki ochrony ... 10*
*8.3. ŚRODKI BEZPIECZEŃSTWA KANAŁÓW ŁĄCZNOŚCI ... 10*
*8.4. ZASADY MONITOROWANIA ORAZ REALIZACJI PRZEGLĄDÓW BEZPIECZEŃSTWA ... 10*
*8.5. PRZYPORZĄDKOWANIE OKREŚLONYCH ŚRODKÓW OCHRONY DO CHRONIONYCH ATRYBUTÓW INFORMACJI. 10*
*8.5.1. Poufność ... 10*
*8.5.2. Dostępność ... 11*
*8.5.3. Integralność danych ... 11*
*8.5.4. Integralność systemu ... 11*
*8.5.5. Uwierzytelnianie ... 11*
*8.5.6. Rozliczalność ... 11*
*8.5.7. Niezaprzeczalność ... 11*
*8.5.8. Inne atrybuty informacji ... 11*
*8.6. OPIS INNYCH ŚRODKÓW OCHRONY ZASOBÓW INFORMACYJNYCH SYSTEMU ... 11*

**9. ADMINISTROWANIE BEZPIECZEŃSTWEM ... 11**

*9.1. PROCEDURY EKSPLOATACYJNE ... 12*
*9.1.1. Procedury związane z eksploatacją systemu ... 12*
*9.1.2. Procedury związane z zarządzaniem użytkownikami systemu ... 12*
*9.1.3. Procedury związane z eksploatacją oprogramowania systemowego ... 12*
*9.1.4. Procedury związane z zarządzaniem siecią teleinformatyczną ... 12*
*9.1.5. Inne procedury związane z bezpieczną eksploatacją systemu ... 12*
*9.2. PROCEDURY AWARYJNE ... 12*
*9.3. ... **Błąd! Nie zdefiniowano zakładki.***
*9.4. ZASADY POSTĘPOWANIA Z DOKUMENTACJĄ SYSTEMU ... 12*
*9.5. ZASADY POSTĘPOWANIA Z DANYMI STANOWIĄCYMI INFORMACJE PRAWNIE CHRONIONE ... 12*
*9.6. PROCEDURY OBSŁUGI PROGRAMÓW MONITORUJĄCYCH ... 12*
*9.7. OPIS INNYCH ZAŁOŻEŃ BEZPIECZNEJ EKSPLOTACJI ... 12*

**10. NARUSZENIE BEZPIECZEŃSTWA INFORMACJI W SYSTEMIE ... 12**

*10.1. ZGŁASZANIE ZDARZEŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM ... 13*
*10.2. ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI ... 13*

**11. ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA SYSTEMU ... 13**

**12. SZKOLENIA ... 13**

**DODATEK A (REALIZACJA WYMAGAŃ I ZALECEŃ BEZPIECZEŃSTWA) ... 13**

**DODATEK B (WYKAZ PROCEDUR) ... 13**

**SPIS RYSUNKÓW ... 13**

**SPIS TABEL ... 13**

## WYKAZ SKRÓTÓW I TERMINÓW

*{W tym punkcie należy przedstawić zastosowane w dokumencie skróty i terminy.}*

## 1. CEL DOKUMENTU

Celem niniejszego dokumentu jest przedstawienie wszelkich zagadnień związanych z bezpieczeństwem systemu/usługi <nazwa systemu/usługi>. Dokument stanowi opis zidentyfikowanych i zastosowanych mechanizmów zapewniających bezpieczeństwo <nazwa systemu/usługi>, w szczególności prezentuje wprowadzone środki ochrony systemu odnoszące się do ochrony fizycznej, zabezpieczeń technicznych, zabezpieczeń informatycznych, łącznie z elementami ochrony kryptograficznej. Ponadto, niniejszy dokument przedstawia obowiązujące uregulowania organizacyjno-prawne mające bezpośrednie zastosowanie w budowaniu bezpieczeństwa <nazwa systemu/usługi> i odnoszące się do wdrożonych środków ochrony.
Informacje zawarte w niniejszym dokumencie są zgodne ze stanem faktycznym środowiska <nazwa systemu/usługi> na dzień <dd.mm.rrrr> r. Wszelkie zmiany w konfiguracji środowiska techniczno-systemowego lub w obszarach organizacyjno-prawnych wpływające na zmianę w podejściu do eksploatowanych środków ochrony systemu lub zmieniające bezpośrednio zastosowane środki ochrony zostaną uwzględnione w kolejnych wersjach „Dokumentacji bezpieczeństwa <nazwa systemu/usługi>".

## 2. ODPOWIEDZIALNOŚĆ

Dokument jest dedykowany wszystkim osobom i podmiotom odpowiedzialnym za realizację projektu <nazwa systemu/usługi> oraz za jego eksploatację.

## 3. ZAKRES I WARUNKI STOSOWANIA DOKUMENTU

Niniejszy dokument określa zasady ochrony informacji przetwarzanych w <nazwa systemu/usługi>, wszystkich zasobów technicznych <nazwa systemu/usługi> oraz obszarów przetwarzania. Określa również zasady postępowania użytkowników <nazwa systemu/usługi>.
Dokument opisuje infrastrukturę sprzętowo-systemową <nazwa systemu/usługi> oraz umiejscowienie <nazwa systemu/usługi> w ramach eksploatowanych w resorcie finansów systemów informatycznych realizujących podstawowe cele biznesowe. Dokument zawiera opis wzajemnych relacji wewnątrz systemu oraz powiązań międzysystemowych z systemami informatycznymi bezpośrednio związanymi z <nazwa systemu/usługi>. Dokument zawiera opis elementów infrastruktury sieciowej, wyłącznie w zakresie pozwalającym na zrozumienie zasad funkcjonowania <nazwa systemu/usługi>, nie zawiera, więc pełnej charakterystyki środowiska sieciowego. W niniejszym dokumencie nie zostały zawarte szczegółowe informacje o systemach współpracujących z <nazwa systemu/usługi> oraz o zastosowanych w nich środkach ochrony.

## 4. POWIĄZANIA Z INNYMI DOKUMENTAMI

*{W tym punkcie należy przedstawić przepisy prawne, dokumenty normatywne, normy, zalecenia techniczne, umowy i inne opracowania związane z bezpieczeństwem systemu/usługi wykorzystane przy opracowaniu dokumentacji bezpieczeństwa systemu.}*

### 4.1. DOKUMENTY USTAWOWE

- …,
- …,

### 4.2. DOKUMENTY NORMATYWNE MINISTERSTWA FINANSÓW

- …,
- …,

### 4.3. NORMY I STANDARDY

- …,
- …,

### 4.4. DOKUMENTACJA SYSTEMU I INNE DOKUMENTY PROJEKTOWE

#### 4.4.1. Dokumentacja systemowa

- …,
- …,

#### 4.4.2. Dokumentacja eksploatacyjna

- …,
- …,

#### 4.4.3. Dokumentacja administracyjna

- …,
- …,

#### 4.4.4. Dokumenty inne

- …,
- …,

## 5. DEFINICJA SYSTEMU

### 5.1. NAZWA SYSTEMU

*{W tym punkcie należy określić nazwę systemu/usługi.}*

### 5.2. PRZEZNACZENIE SYSTEMU

*{W tym punkcie należy opisać cele realizacji projektu.}*

### 5.3. LOKALIZACJA SYSTEMU

*{W tym punkcie należy opisać, w jakich lokalizacjach system będzie zainstalowany i eksploatowany.}*

### 5.4. MIEJSCE SYSTEMU W INFRASTRUKTURZE INFORMATYCZNEJ RESORTU FINANSÓW

*{W tym punkcie należy opisać miejsce systemu w istniejącej infrastrukturze informatycznej resortu finansów (z uwzględnieniem instalacji szkoleniowych, testowych i deweloperskich).}*

### 5.5. PODMIOTY ODPOWIEDZIALNE ZA SYSTEM ORAZ JEGO EKSPLOATACJĘ

*{W tym punkcie należy opisać zakres odpowiedzialności za eksploatację systemu/usługi według następującego wzoru:}*

| NAZWA PODMIOTU | OPIS ZAKRESU ODPOWIEDZIALNOŚCI |
|---|---|
| Właściciel systemu | |
| | |
| Komórki organizacyjne Ministerstwa Finansów | |
| | |
| | |
| Inne jednostki organizacyjne resortu finansów | |
| | |
| | |
| Firmy zewnętrzne | |
| | |
| | |
| Użytkownicy/jednostki zewnętrzne | |
| | |
| | |
| Inne podmioty odpowiedzialne za system | |
| | |

### 5.6. ODBIORCY SYSTEMU

*{W tym punkcie należy opisać wszystkich odbiorców systemu z uwzględnieniem wszystkich aspektów dotyczących wykorzystywania systemu, jego bieżącej eksploatacji oraz utrzymania funkcjonalności zgodnej z obowiązującymi przepisami prawa.}*

## 6. OPIS SYSTEMU

### 6.1. CHARAKTERYSTYKA I KLASYFIKACJA INFORMACJI W SYSTEMIE

*{W tym punkcie należy opisać i przedstawić klasyfikację informacji przetwarzanych w systemie w podziale na:*
- *informację operacyjną,*
- *informację techniczną,*
- *informacje prawnie chronione - należy załączyć wykaz wymaganej dokumentacji dla poszczególnych grup informacji przetwarzanych w systemie.}*

### 6.2. ARCHITEKTURA LOGICZNA SYSTEMU

*{W tym punkcie należy opisać wydzielone w ramach architektury logicznej systemu warstwy wraz z załączonym graficznym przedstawieniem modelu logicznego systemu z umiejscowieniem poszczególnych warstw.}*

#### 6.2.1. Warstwa interfejsu użytkownika

#### 6.2.2. Warstwa kontroli dostępu

#### 6.2.3. Warstwa aplikacji

#### 6.2.4. Warstwa bazy danych

#### 6.2.5. Inne warstwy

### 6.3. PRZEPŁYW DANYCH I INFORMACJI W SYSTEMIE

*{W tym punkcie należy przedstawić koncepcję obiegu informacji i danych w systemie wraz z załączonym przedstawieniem graficznym.}*

### 6.4. ARCHITEKTURA FIZYCZNA SYSTEMU

*{W tym punkcie należy przedstawić ogólny opis systemu wraz z załączonym graficznym przedstawieniem architektury fizycznej systemu z uwzględnieniem następujących elementów:}*

#### 6.4.1. Infrastruktura serwerowa z podziałem na realizowane funkcje

#### 6.4.2. Inne komponenty sprzętowe

#### 6.4.3. Połączenia i zależności pomiędzy poszczególnymi elementami

#### 6.4.4. Połączenia sieciowe

#### 6.4.5. Architektura środowiska sieciowego WAN/LAN

#### 6.4.6. System tworzenia kopiowania zabezpieczającego

#### 6.4.7. System monitorowania pracy systemu

#### 6.4.8. Wykorzystywane oprogramowanie systemowe i narzędziowe wraz z jego umiejscowieniem

#### 6.4.9. Wykorzystywane oprogramowanie użytkowe wraz z jego umiejscowieniem

#### 6.4.10. Wymagania sprzętowo-systemowe dla użytkownika końcowego

### 6.5. PODZIAŁ RÓL W SYSTEMIE (REALIZACJI USŁUGI)

*{W tym punkcie należy opisać role wyodrębnione w zależności od rodzaju poszczególnych modułów i aplikacji wchodzących w skład systemu. Poza rolami związanymi bezpośrednio z funkcjonalnością merytoryczną systemu należy również opisać role w obszarze technicznym, związane z obsługą infrastruktury sprzętowo-systemowej, a także z inspekcją bezpieczeństwa systemu. Należy określić dla poszczególnych ról:*

- *jakie muszą spełniać wymagania,*
- *jakie mają obowiązki i zakres odpowiedzialności,*
- *jaki poziom uprawnień,*
- *kto jest odpowiedzialny za wyznaczanie osób do pełnienia roli itp.}*

| NAZWA ROLI | OPIS |
|---|---|
| **Administrator aplikacji** | |
| Główne obowiązki: | |
| Zakres odpowiedzialności: | |
| Wymagania: | |
| Poziom uprawnień: | |
| Odpowiedzialny za wyznaczenie: | |
| Inne uwagi: | |
| **Użytkownik** | |
| Główne obowiązki: | |
| Zakres odpowiedzialności: | |
| Wymagania: | |
| Poziom uprawnień: | |
| Odpowiedzialny za wyznaczenie: | |
| Inne uwagi: | |
| **Użytkownik zewnętrzny** | |
| Główne obowiązki: | |
| Zakres odpowiedzialności: | |
| Wymagania: | |
| Poziom uprawnień: | |
| Odpowiedzialny za wyznaczenie: | |
| Inne uwagi: | |
| **Administrator serwera aplikacji** | |
| Główne obowiązki: | |
| Zakres odpowiedzialności: | |
| Wymagania: | |
| Poziom uprawnień: | |
| Odpowiedzialny za wyznaczenie: | |
| Inne uwagi: | |
| **Administrator sieci teleinformatycznej** | |
| Główne obowiązki: | |
| Zakres odpowiedzialności: | |
| Wymagania: | |
| Poziom uprawnień: | |
| Odpowiedzialny za wyznaczenie: | |
| Inne uwagi: | |

| **Inspektor bezpieczeństwa** | |
|---|---|
| Główne obowiązki: | |
| Zakres odpowiedzialności: | |
| Wymagania: | |
| Poziom uprawnień: | |
| Odpowiedzialny za wyznaczenie: | |
| Inne uwagi: | |
| **Inne role** | |
| Główne obowiązki: | |
| Zakres odpowiedzialności: | |
| Wymagania: | |
| Poziom uprawnień: | |
| Odpowiedzialny za wyznaczenie: | |
| Inne uwagi: | |

### 6.6. ZABEZPIECZENIA KRYPTOGRAFICZNE

*{W tym punkcie należy opisać zastosowane w systemie rozwiązania kryptograficzne oraz rodzaje wykorzystywanych certyfikatów.}*

#### 6.6.1. Polityka wykorzystania zabezpieczeń kryptograficznych

#### 6.6.2. Rodzaje wykorzystywanych certyfikatów

#### 6.6.3. Zasady zarządzanie kluczami

## 7. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

*{Krytyczne lub wrażliwe środki przetwarzania informacji należy umieszczać w obszarach bezpiecznych, chronionych fizyczną granicą przez odpowiednie bariery bezpieczeństwa oraz zabezpieczenia wejścia. W tym punkcie należy opisać obszary bezpieczne oraz ich granice, stosowane w celu ochrony informacji i środków przetwarzania informacji dla danego systemu oraz w jaki sposób odbywa się ochrona fizyczna przed nieuprawnionym dostępem fizycznym, uszkodzeniami lub zakłóceniami pracy. W szczególności należy określić:}*

### 7.1. ELEMENTY ELEKTRONICZNEGO ŚRODOWISKA BEZPIECZEŃSTWA

#### 7.6.1. Interfejsy człowiek-sprzęt wykorzystywane w systemie

#### 7.6.2. Interfejsy pomiędzy elementami systemu o różnych klasach bezpieczeństwa

#### 7.6.3. Interfejsy do innych systemów

#### 7.6.4. Zasady podłączenia do zewnętrznych sieci łączności

#### 7.6.5. Inne elementy elektronicznego środowiska bezpieczeństwa

# 8. ŚRODKI OCHRONY ZASOBÓW INFORMACYJNYCH SYSTEMU

*{W tym punkcie należy przedstawić środki, które zastosowano w systemie dla ograniczenia ryzyka wystąpienia zdarzeń negatywnie wpływających na bezpieczeństwo informacji w nim przetwarzanych.}*

## 8.1. ORGANIZACYJNE I PRAWNE ŚRODKI OCHRONY

*{Akty normatywne, regulaminy, struktury organizacyjne, ścieżki raportowania itp., mające na celu zapewnienie bezpieczeństwa systemu.}*

## 8.2. INFORMATYCZNE ŚRODKI OCHRONY

*{Wszelkie rozwiązania informatyczne stanowiące integralną część którejkolwiek z warstw systemu takie, jak:}*

### 8.2.1. Środki ochrony przed awarią systemu

#### 8.2.1.1 Środki ochrony przed awarią ośrodków i węzłów

*{Opisać np. wykorzystywane zapasowe ośrodki przetwarzania, środki ochrony dla węzłów sieci, środki ochrony dla serwerów, zastosowane redundancje elementów systemu itp.}*

#### 8.2.1.2 Środki ochrony przed awarią nośników danych i zespołów nośnikow danych

*{Opisać zastosowany system wykonywania kopii zapasowych, zastosowane macierze dyskowe, zasady replikacji danych itp.}*

#### 8.2.1.3 Środki ochrony przed awarią infrastruktury sieciowej

*{Opisać środki ochrony dla sieci LAN/WAN, zastosowane redundancje elementów sieciowych, awaryjne kanały dostępu itp.}*

### 8.2.2. Środki ochrony konfiguracji systemu

*{Opisać zastosowane środki ochrony plików systemowych serwerów, konfiguracji systemu np. przed złośliwym oprogramowaniem itp.}*

### 8.2.3. Środki ochrony dostępu do systemu

*{Opisać zastosowane środki ochrony dostępu dla użytkowników wewnętrznych i zewnętrznych oraz użytkowników o podwyższonych uprawnieniach (np. administratorów).}*

### 8.2.4. Środki ochrony integralności danych

*{Opisać zastosowane środki ochrony integralności danych na poziomie serwera bazy danych, aplikacji np. zasady walidacji danych, spójności słowników bazy danych itp.}*

### 8.2.5. Inne informatyczne środki ochrony

*{Opisać zastosowane inne informatyczne środki ochrony np. ślad rewizji na poziomie aplikacji, śledzenie zmian w bazie danych, śledzenie zmian na poziomie systemu operacyjnego serwera itp.}*

## 8.3. ŚRODKI BEZPIECZEŃSTWA KANAŁÓW ŁĄCZNOŚCI

*{Rozwiązania służące ochronie poufności i dostępności kanałów komunikacyjnych, np. poprzez szyfrowanie kanałów, redundancję.}*

## 8.4. ZASADY MONITOROWANIA ORAZ REALIZACJI PRZEGLĄDÓW BEZPIECZEŃSTWA

*{Rozwiązania administracyjne oparte o mechanizmy informatyczne służące do wykrywania sytuacji zagrażającej bezpieczeństwu systemu, zapewniające integralność aktualnej konfiguracji poszczególnych warstw systemu oraz badaniu skuteczności przyjętych środków ochrony.}*

## 8.5. PRZYPORZĄDKOWANIE OKREŚLONYCH ŚRODKÓW OCHRONY DO CHRONIONYCH ATRYBUTÓW INFORMACJI.

### 8.5.1. Poufność

Właściwość danych wskazująca obszar, w którym te dane nie powinny być dostępne lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom. Środki realizujące ochronę poufności to:

- …,
- …,

8.5.2. Dostępność

Zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne. Środki realizujące ochronę dostępności to:
- …,
- …,

8.5.3. Integralność danych

Właściwość polegająca na tym, że dane nie zostały wcześniej zmienione lub zniszczone w nieautoryzowany sposób. Środki realizujące ochronę integralności danych to:
- …,
- …,

8.5.4. Integralność systemu

Właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej. Środki realizujące ochronę integralności systemu to:
- …,
- …,

8.5.5. Uwierzytelnianie

Uwierzytelnienie definiowane jest jako zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana. Środki realizujące ochronę uwierzytelniania to:
- …,
- …,

8.5.6. Rozliczalność

Rozliczalność jest definiowana jako właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi. Środki realizujące ochronę rozliczalności to:
- …,
- …,

8.5.7. Niezaprzeczalność

Niezaprzeczalność jest definiowana jako właściwość zapewniająca, że autor danej transakcji nie może się wyprzeć faktu jej dokonania. Środki realizujące ochronę niezaprzeczalności to:
- …,
- …,

8.5.8. Inne atrybuty informacji

8.6. OPIS INNYCH ŚRODKÓW OCHRONY ZASOBÓW INFORMACYJNYCH SYSTEMU.

## 9. ADMINISTROWANIE BEZPIECZEŃSTWEM

*{Administrowanie bezpieczeństwem systemu ma na celu utrzymanie zakładanego poziomu bezpieczeństwa przetwarzanych w systemie informacji, obejmującego aspekty dostępności, integralności i poufności. Wszystkie czynności dotyczące systemu, wykonywane przez administratorów, użytkowników i osoby postronne (np. serwis) muszą być ujęte w procedury, zapewniające możliwość wykonania przez wykwalifikowany personel.*
*W tym punkcie należy opisać zasady eksploatacji systemu i jego administrowania, gwarantujące utrzymanie bezpieczeństwa, należy opisać wszystkie procedury związane z przetwarzaniem danych oraz warunkami technicznymi i organizacyjnymi, jakimi powinny odpowiadać urządzenia i systemy.*
*Procedury powinny być opracowane z uwzględnieniem obowiązujących w Ministerstwie Finansów standardów i wzorców. Należy określić założenia dokumentowania i wprowadzania w życie procedur dla systemu.*

*Procedury związane z systemem można podzielić na dwie grupy:*
- *procedury dedykowane, opracowane na potrzeby tego systemu,*
- *procedury uniwersalne, obowiązujące w resorcie, mające zastosowanie dla innych systemów lub elementów infrastruktury sprzętowo-systemowej.*

*Założenia do procedur i procedury powinny zostać opracowane w następujących grupach:}*

### 9.1. PROCEDURY EKSPLOATACYJNE

#### 9.1.1. Procedury związane z eksploatacją systemu

*{Procedury związane z eksploatacją systemu, instalacją i modyfikacją oprogramowania, tworzeniem kopii zapasowych danych, konfiguracji parametrów aplikacji itp.}*

#### 9.1.2. Procedury związane z zarządzaniem użytkownikami systemu

*{Procedury dotyczące rejestracji użytkowników, zarządzania uprawnieniami, hasłami użytkowników itp.}*

#### 9.1.3. Procedury związane z eksploatacją oprogramowania systemowego

*{Procedury dotyczące instalacji i modyfikacji oprogramowania systemowego i narzędziowego, procedury postępowania z hasłami systemowymi, tworzenia nośników ratunkowych dla systemów, prowadzenia dzienników systemowych itp.}*

#### 9.1.4. Procedury związane z zarządzaniem siecią teleinformatyczną

*{Procedury związane z zarządzaniem urządzeniami aktywnymi, zarządzaniem konfiguracją sieci, monitorowaniem pracy sieci itp.}*

#### 9.1.5. Inne procedury związane z bezpieczną eksploatacją systemu

*{Np. procedury związane z udostępnianiem i przekazywaniem sprzętu komputerowego do naprawy, niszczeniem nośników, zarządzaniem wymiennymi nośnikami danych, zabezpieczeniem przed kodem złośliwym oraz kodem mobilnym, bezpiecznym usuwaniem informacji na nośnikach i wydrukach itp.}*

### 9.2. PROCEDURY AWARYJNE

*{Procedury, które należy wykonywać w przypadku wystąpienia sytuacji awaryjnych w pracy systemu np.: odtwarzania danych z kopii zapasowych, postępowania w przypadku awarii sprzętowej itp.}*

### 9.3.

### 9.4. ZASADY POSTĘPOWANIA Z DOKUMENTACJĄ SYSTEMU

### 9.5. ZASADY POSTĘPOWANIA Z DANYMI STANOWIĄCYMI INFORMACJE PRAWNIE CHRONIONE

*{Dotyczy np. danych stanowiących tajemnicę skarbową lub danych osobowych.}*

### 9.6. PROCEDURY OBSŁUGI PROGRAMÓW MONITORUJĄCYCH

### 9.7. OPIS INNYCH ZAŁOŻEŃ BEZPIECZNEJ EKSPLOTACJI

Szczegółowy wykaz procedur jest określony w Dodatku B.

## 10. NARUSZENIE BEZPIECZEŃSTWA INFORMACJI W SYSTEMIE

*{W tym punkcie należy opisać zastosowane mechanizmy związane z zarządzaniem incydentami związanymi z bezpieczeństwem informacji w systemie. Naruszenie bezpieczeństwa informacji to wszelkie mogące mieć miejsce zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę naruszenia lub utraty zasobów, utraty poufności lub integralności, ograniczenia dostępności informacji lub zmniejszenia niezawodności systemów. Naruszeniem bezpieczeństwa są także odstępstwa od obowiązujących procedur postępowania, nawet, jeżeli nie prowadzą do wyżej wymienionych skutków.*
*Należy opisać procedury dotyczące zgłaszania incydentów, ich dokumentowania oraz zasady analizowania i reagowania na incydenty.}*

10.1. ZGŁASZANIE ZDARZEŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM

10.2. ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI

## 11. ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA SYSTEMU

*{W tym punkcie zależy opisać jakie zostały opracowane dokumenty związane z zarządzeniem ciągłością działania systemu w celu przeciwdziałania przerwom w działalności biznesowej oraz ochronie krytycznych procesów biznesowych przed rozległymi awariami lub katastrofami oraz zapewnienia wznowienia działalności w wymaganym czasie np.:*
*– wykaz krytycznych procesów biznesowych zależnych od działania systemu,*
*– plan ciągłości,*
*– procedura testowania planu ciągłości,*
*– zasady i procedura aktualizacji planu ciągłości działania.}*

## 12. SZKOLENIA

*{Wszyscy użytkownicy pracujący z systemem powinni zostać przeszkolenie w zakresie bezpiecznej eksploatcji systemu oraz z być zapoznani z obowiązującymi regulacjami prawnymi dotyczącymi ochrony danych i systemów informatycznych. Każdy użytkownik powinien posiadać wiedzę adekwatną do swego zakresu obowiązków, wykonywanych zadań i przypisanego zakresu odpowiedzialności.*
*W tym punkcie należy opisać wymagane szkolenia związane z wdrożeniem i eksploatacją systemu dla grup pracowniczych (np. użytkowników, administratorów, kierowników jednostek) w zakresie:*
*– eksploatacji systemu,*
*– bezpieczeństwa danych i systemu.*
*Należy opisać również wymaganą infrastrukturę i materiały szkoleniowe (bazy szkoleniowe, scenariusze, podręczniki) potrzebne do realizacji szkoleń. Należy określić czy przeszkolenie jest warunkiem koniecznym do dopuszczenia pracownika do użytkowania systemu i przetwarzania informacji.*
*Należy również opisać inne metody wspomagania użytkownika w zakresie bezpiecznej eksploatacji takie, jak np.: usługa Help Desk, infolinia, podręczniki elektroniczne itp.}*

## DODATEK A (REALIZACJA WYMAGAŃ I ZALECEŃ BEZPIECZEŃSTWA)

Według wzoru

| LP | NAZWA WYMAGANIA LUB ZALECENIA | SPOSÓB REALIZACJI |
|---|---|---|
| | | |

## DODATEK B (WYKAZ PROCEDUR)

Według wzoru

| LP | NAZWA PROCEDURY | IDENTYFIKATOR PROCEDURY |
|---|---|---|
| | | |

## SPIS RYSUNKÓW

## SPIS TABEL