

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

Z A T W I E R D Z A M

.....
data *podpis, pieczęć*

| |
|--|
| <p>DOKUMENT GŁÓWNY</p> |
| <p>POLITYKA BEZPIECZEŃSTWA INFORMACJI DLA KRAJOWEGO SYSTEMU INFORMATYCZNEGO SIMIK 07-13</p> |

| | | | |
|--|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

Historia zmian

| <i>Nr wersji</i> | <i>Data</i> | <i>Autorzy</i> | <i>Opis zmian</i> |
|------------------|------------------|--|---|
| 0.8 | 25.06.2007 | Piotr Łoziński Andrzej Oszmian | Utworzenie nowego dokumentu |
| 1.0 | 25.10.2007 | Piotr Łoziński Andrzej Oszmian | Zatwierdzona przez Dyrektora Departamentu MF/RI |
| 1.2 | 25.02.2008 | Waldemar Gaik Piotr Łoziński Andrzej Oszmian | Ujednolicono procedury i nazewnictwo wypracowane wspólnie przez MF i MRR |
| | 29.02.2008 | | Zatwierdzona przez Kierownika Projektu |
| | 29.02.2008 | | Zatwierdzona przez Dyrektora Departamentu MF/RI |
| 1.3 | 28.04.2008 | Andrzej Oszmian | Zmiana numeracji załączników tego dokumentu. Dodano załączniki: upoważnienie do pełnienia funkcji ABI oraz ZBI |
| | 28.04.2008 | | Zatwierdzona przez Dyrektora Departamentu MF/RI |
| 1.4 | 10.07.2008 | Grzegorz Brandebura | Usunięto zapis z pkt. 12.1 dotyczący ustalania harmonogramu przestrzegania zasad PBI |
| 2.0 | 10.10.2008 | Grzegorz Brandebura | Gruntowne przekonstruowanie dokumentu, zdjęcie klauzuli: „zastrzeżone do użytku służbowego w MF i MRR” |
| | 21.10-07.11.2008 | Waldemar Gaik | 1. Usunięto rolę Koordynatora SIMIK, zastąpił a go rola Administratora Merytorycznego 2. Wprowadzenie uwag |
| | 10-18.11.2008 | Stach Leszczyński | 3. Weryfikacja – wprowadzenie uwag |
| 2.1 | 15-19.12.2008 | Grzegorz Brandebura | 1. Weryfikacja uwag wprowadzonych przez MRR. |

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

I. Spis treści

| | | |
|--------|---|----|
| I. | Spis treści | 3 |
| II. | Wstęp | 4 |
| III. | Cel polityki bezpieczeństwa..... | 5 |
| IV. | Opis i zasięg systemu..... | 6 |
| V. | Zasoby KSI SIMIK 07-13 | 7 |
| VI. | Obszary przetwarzania informacji..... | 8 |
| VII. | Analiza ryzyka..... | 9 |
| VIII. | Hierarchia ról i zadań w KSI SIMIK 07-13 | 10 |
| IX. | Organizacja bezpieczeństwa..... | 13 |
| X. | Bezpieczeństwo osobowe..... | 15 |
| 1. | Zasady postępowania użytkowników | 15 |
| 2. | Szkolenia użytkowników | 15 |
| XI. | Bezpieczeństwo fizyczne i środowiskowe głównej infrastruktury systemu | 16 |
| XII. | Zarządzanie systemem i siecią dla głównej infrastruktury systemu..... | 17 |
| 1. | Zarządzanie serwerami | 17 |
| 2. | Zarządzanie siecią..... | 18 |
| XIII. | Kontrola dostępu..... | 20 |
| 1. | Dostęp użytkowników do systemu | 20 |
| 2. | Polityka haseł..... | 20 |
| XIV. | Monitorowanie bezpieczeństwa | 22 |
| XV. | Naruszenia bezpieczeństwa..... | 23 |
| XVI. | Rozwój systemu..... | 24 |
| XVII. | Zarządzanie ciągłością działania | 25 |
| XVIII. | Szkolenia | 26 |
| XIX. | Słownik pojęć | 27 |
| XX. | Załączniki | 28 |
| 1. | Załącznik 1. Wzór upoważnienia oraz zadania AT..... | 28 |
| 2. | Załącznik 2. Wzór upoważnienia oraz zadania AM IK NSRO..... | 30 |
| 3. | Załącznik 3. Wzór odwołania osoby z pełnienia funkcji AM IK NSRO..... | 31 |
| 4. | Załącznik 4. Wzór upoważnienia oraz zadania AM IZ | 32 |
| 5. | Załącznik 5. Wzór odwołania osoby z pełnienia funkcji AM IZ | 33 |
| 6. | Załącznik 6. Wzór upoważnienia oraz zadania AM I w Instytucji | 34 |
| 7. | Załącznik 7. Wzór odwołania osoby z pełnienia funkcji AM I..... | 35 |
| 8. | Załącznik 8. Raporty z monitorowania bezpieczeństwa IT | 36 |
| 9. | Załącznik 9. Wzór upoważnienia osoby do pełnienia funkcji ABI..... | 37 |
| 10. | Załącznik 10. Wzór upoważnienia osoby do pełnienia funkcji członka ZBI..... | 38 |

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

II. Wstęp

KSI SIMIK 07-13, powstał aby zapewnić monitoring funduszy strukturalnych w nowej perspektywie finansowania w latach 2007 – 2013. Formułowanie zasad bezpieczeństwa w niniejszym dokumencie i dokumentach związanych ma na celu zapewnienie dostępności, integralności, rozliczalności informacji zawartych w systemie.

Rada Projektu SIMIK deklaruje swoje zaangażowanie dla działań zapewniających bezpieczeństwa informacji przetwarzanych w systemie KSI SIMIK 07-13.

Niniejszy dokument Polityki bezpieczeństwa KSI SIMIK 07-13, porządkuje kwestie związane z bezpieczeństwem informacji w KSI SIMIK 07-13, oraz zawiera najważniejsze zasady postępowania z informacją.

Jest to dokument jawny, z którym zapoznać powinni się wszyscy użytkownicy systemu KSI SIMIK 07-13.

Właścicielem Polityki bezpieczeństwa jest Ministerstwo Rozwoju Regionalnego jako główny użytkownik systemu.

Obowiązkiem użytkowników systemu jest przestrzeganie zasad ustanowionych w niniejszej polityce bezpieczeństwa, tak aby zapewniać odpowiedni poziom bezpieczeństwa informacji, oraz utrzymanie ciągłości dostępu do informacji.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

III. Cel polityki bezpieczeństwa

Celem polityki bezpieczeństwa informacji dla KSI SIMIK 07-13 jest zdefiniowanie zasad, metod i środków ochrony informacji w systemie. Zapewnienie ich **dostępności** dla wszystkich uprawnionych osób zawsze gdy zachodzić będzie taka potrzeba, **integralności** informacji tzn. że nie będą one modyfikowane przez nieuprawnione osoby co prowadziłyby do ich fałszowania, oraz zachowania rozliczalności informacji, tzn. możliwości sprawdzenia kto dopisywał, modyfikował, czy usuwał dane..

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

IV. Opis i zasięg systemu

KSI SIMIK 07-13 jest systemem o zasięgu ogólnokrajowym dostępnym przez Internet. KSI SIMIK 07-13 zawiera funkcjonalność wspomagającą proces programowania i monitorowania wdrażania realizowanych projektów UE w Polsce. Podmiotami uczestniczącymi w systemie są:

- a. MRR –IK NSRO– departament w MRR pełniący rolę IK NSRO– Administratorzy Merytoryczni IK NSRO
- b. Instytucje zarządzające (IZ) poszczególnymi programami operacyjnymi - Administratorzy Merytoryczni IZ
- c. Instytucje uczestniczące we wdrażaniu poszczególnych programów operacyjnych - Administratorzy Merytoryczni w Instytucji
- d. MF RI – Departament Rozwoju Systemów Informatycznych w MF
- e. Instytucje – Użytkownicy systemu – instytucje zarządzające, pośredniczące, Instytucje Certyfikujące, Instytucja Audytowa.

KSI SIMIK 07-13 nie jest systemem mającym krytyczne znaczenie dla instytucji go użytkujących. Jest to system wspomagający, zapewniający ewidencjonowanie informacji związanych z projektami na dofinansowanie przez Unię Europejską, inwestycji czy działań wykonywanych na terenie Polski.

Powiązania KSI SIMIK 07-13 z innymi systemami obrazuje załącznik 5.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

V. Zasoby KSI SIMIK 07-13

Ochronie podlegają zasoby związane z przetwarzaniem informacji w KSI SIMIK 07-13. Wykaz zasobów systemu podano w Instrukcji zarządzania Krajowym Systemem Informatycznym SIMIK07-13 (PBI-IZS).

Szczegółnej ochronie podlega Główna infrastruktura KSI SIMIK 07-13.

KSI SIMIK07-13 składa się z elementów wymienionych w Instrukcji zarządzania Krajowym Systemem Informatycznym SIMIK 07-13 (PBI-IZS).

Instrukcja zarządzania Krajowym Systemem Informatycznym SIMIK 07-13 oraz dokumentacja techniczna KSI SIMIK 07-13 są aktualizowane zgodnie z ustaleniami przyjętymi w dokumencie „Zasady aktualizacji dokumentacji bezpieczeństwa KSI SIMIK 07-13”.

Weryfikacja i przeprowadzanie analizy ryzyka dla KSI SIMIK 07-13, odbywa się zgodnie z dokumentem „Zasady aktualizacji dokumentacji bezpieczeństwa KSI SIMIK 07-13”.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

VI. Obszary przetwarzania informacji

1. Dostęp do systemu KSI SIMIK 07-13, możliwy jest poprzez łącza internetowe, tak więc zalogowanie się do systemu i przetwarzanie informacji w systemie umożliwia każdy komputer:
 - wyposażony w odpowiednią wersję przeglądarki internetowej (z uwzględnieniem wymaganych ustawień). Informacje o wymaganych przeglądarkach, ich wersjach i ustawieniach dostępne są na stronach internetowych MRR.
 - podłączony do Internetu.
2. Komputery klienckie użytkowników powinny być chronione zgodnie z dokumentem „Zalecenia dotyczące zabezpieczenia komputerów użytkowników” a także politykami bezpieczeństwa wewnątrz instytucji, które użytkują system.
3. Podstawowym obszarem przetwarzania informacji jest serwerownia KSI SIMIK 07-13, zapewniająca pracę i ochronę głównej infrastruktury systemu.
4. Komunikacja z systemem odbywa się przy użyciu połączenia szyfrowanego (https), przy użyciu protokołu SSL.

| | | | |
|--|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

VII. Analiza ryzyka

Weryfikacja i przeprowadzanie analizy ryzyka dla KSI SIMIK 07-13, odbywa się zgodnie z dokumentem „Zasady aktualizacji dokumentacji bezpieczeństwa KSI SIMIK 07-13”. Dla przeprowadzenia analizy ryzyka sporządzany jest oddzielny dokument „Analiza ryzyka dla KSI SIMIK 07-13”.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

VIII. Hierarchia ról i zadań w KSI SIMIK 07-13

Głównym Użytkownikiem KSI SIMIK 07-13 jest Ministerstwo Rozwoju Regionalnego(MRR). Głównym Dostawcą jest Departament Informatyki Ministerstwa Finansów (DI/MF).

MRR odpowiada m.in. za zarządzanie, nadawanie uprawnień wszystkim AM i Użytkownikom oraz za współpracę z Instytucjami korzystającymi z KSI SIMIK 07-13. MF odpowiada za zarządzanie i współpracę z Koordynatorami SIMIK którzy jednocześnie pełnią rolę Administratora Merytorycznego w systemie KSI SIMIK 07-13.

1. Użytkownicy:

Głównym Użytkownikiem jest Ministerstwo Rozwoju Regionalnego. Użytkowników i zakres ich uprawnień w określonym programie operacyjnym wyznaczają poszczególne instytucje zarządzające, na podstawie zgłoszeń od instytucji pośredniczących. Liczba Instytucji zaangażowanych w proces zarządzania i kontroli w okresie programowania 2007-2013 wynosi ok. 120, co pozwala ocenić, że liczba Użytkowników (osób) bezpośrednio wykorzystujących system kształtować się będzie w przedziale 3500 - 4500. Docelowo system powinien obsługiwać do 1000 Użytkowników jednocześnie.

Użytkownikami systemu zarządzają AM IK NSRO wyznaczeni przez Ministerstwo Rozwoju Regionalnego oraz AM IZ wyznaczeni przez Instytucje Zarządzające i AM I wyznaczeni przez pozostałe Instytucje korzystające z KSI SIMIK 07-13.

2. Administratorzy:

2.1 AI

Rolę AI pełni z-ca dyrektora MF/DI, nadzorujący projekt SIMIK. Do zadań AI należy:

- a) wyznaczenie osób pełniących rolę ABI
- b) wyznaczenie osób pełniących rolę AT
- c) wyznaczenie członków ZBI
- d) powołanie w porozumieniu z MRR członków ZK
- e) analiza raportów otrzymywanych od ABI

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

- f) powołanie dodatkowej komisji do przeprowadzenia postępowania wyjaśniającego w celu pełnego zbadania przyczyn i skutków incydentu, ustalenia sprawcy oraz wielkości poniesionych strat
- g) określanie innych zadań związanych dotyczących Polityki Bezpieczeństwa i wyznaczenie do tych zadań osób

AI może wyznaczyć na piśmie inną osobę pełniącą funkcję AI spośród kierownika Projektu lub zastępcy kierownika Projektu

2.2 ABI

Osoba lub zespół powołany przez AI do zadań związanych z ochroną KSI SIMIK 07-13 w szczególności:

- a) reagowanie na incydenty zgodnie z „Instrukcją postępowania ABI w sytuacji naruszenia bezpieczeństwa informacji”,
- b) analiza i ewidencjowanie incydentów,
- c) koordynowanie działań związanych z bezpieczeństwem informacji KSI SIMIK 07-13,
- d) opracowywanie i aktualizacja dokumentacji bezpieczeństwa KSI SIMIK 07-13
- e) inne zadania związane z ochroną systemu wyznaczone przez AI.

2.3 AT

Osoba/osoby wyznaczona przez AI do zarządzania KSI SIMIK 07-13, w szczególności administracja serwerami aplikacyjnymi i bazodanowymi oraz urządzeniami sieciowymi należącymi do systemu. AT nie zarządza kontami Użytkowników. Wzór upoważnienia oraz szczegółowe zadania AT określone są w załączniku 1.

2.4 AM IK NSRO

Osoba/osoby wyznaczona przez MRR do zarządzania Użytkownikami (zakładanie/usuwanie kont Użytkowników, przyznawanie/odbieranie uprawnień Użytkowników). Wzór

| | | | |
|--|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

upoważnienia oraz zadania AM IK NSRO określone są w załączniku 2.

2.5 AM IZ

Osoba/osoby wyznaczona przez Instytucję Zarządzającą do zarządzania Użytkownikami. Wzór upoważnienia oraz zadania AM IZ określone są w załączniku 3.

2.6 AM I

Osoba/osoby wyznaczona przez Instytucję do zarządzania Użytkownikami. Wzór upoważnienia oraz zadania AM I określone są w załączniku 4.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

IX. Organizacja bezpieczeństwa

1. Powołuje się **Administradora Bezpieczeństwa Informacji (ABI)** w celu realizacji zadań związanych z ochroną informacji w KSI SIMIK 07-13, a w szczególności:
 - a) reagowanie na incydenty zgodnie z „Instrukcją postępowania ABI w sytuacji naruszenia bezpieczeństwa informacji”,
 - b) analiza i ewidencjonowanie incydentów,
 - c) koordynowanie działań związanych z bezpieczeństwem informacji KSI SIMIK 07-13,
 - d) opracowywanie i aktualizacja dokumentacji bezpieczeństwa KSI SIMIK 07-13
 - e) inne zadania związane z ochroną systemu wyznaczone przez AI.

Wzór upoważnienia stanowi załącznik 7.

2. Powołuje się **Zespół ds. Spraw Bezpieczeństwa Informacji (ZBI)** w celu zapewnienia koordynacji i kontrolowania procesu bezpieczeństwa w tym także opracowywania i aktualizacji dokumentacji bezpieczeństwa KSI SIMIK 07-13. W skład zespołu wchodzi: Administrator Bezpieczeństwa Informacji (ABI), Administrator/Administratorzy techniczni (AT), Kierownik Projektu (KP), przedstawiciel/przedstawiciele Głównego Użytkownika (Ministerstwa Rozwoju Regionalnego)..
3. Powołuje się **Zespół Kryzysowy (ZK)** w celu podjęcia działań w sytuacjach kryzysowych, np. poważnej awarii systemu (zagrożenie braku dostępności systemu na czas dłuższy niż 12 godzin) tak aby zapewnić ciągłość działania KSI, wystąpienia kompromitacji (np. utraty prawidłowych właściwości działania systemu, co spowodowałyby konsekwencje polityczne, medialne) KSI SIMIK 07-13. W skład zespołu powinni wchodzić następujące osoby:
 - Przedstawiciel(e) MF,
 - Przedstawiciel(e) MRR,

Zespół może powołać na zasadzie ekspertów osoby z biura informacji niejawnych MF/MRR, osoby z biura prasowego MF/MRR, osoby z departamentu prawnego MF/MRR.

Członkowie ZK wybierają spośród siebie Koordynatora ZK oraz jego zastępcę, którzy pełnią

| | | | |
|--|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

funkcje organizacyjne związane z pracami ZK, np. przewodniczenie posiedzeniom, pisanie protokołów lub notatek z posiedzeń, informowanie pozostałych członów ZK o terminach posiedzeń.

Informacje na temat sposobu powiadamiania członków zespoły, trybu i okoliczności powodujących ustalanie terminów spotkań, znajdują się w dokumencie: „Plan ciągłości działania Krajowego Systemu Informatycznego SIMIK 07-13”. Dokument przeznaczony jest do wiadomości członków ZK. Imienny spis członków ZK, dane kontaktowe oraz zakres ich zadań znajduje się w dokumencie: „Zakresy zadań i dane kontaktowe ZK”.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

X. Bezpieczeństwo osobowe

1. Zasady postępowania użytkowników

- a) Użytkownicy KSI SIMIK 07-13, muszą zachowywać w tajemnicy informacje umożliwiające logowanie do systemu;
- b) Użytkownicy są zobowiązani do okresowej zmiany haseł dostępu do systemu, nie rzadziej jednak niż raz na 30 dni;
- c) Użytkownicy są zobowiązani do przestrzegania odpowiednich instrukcji, wytycznych, zaleceń dotyczących pracy w KSI SIMIK 07-13, tak aby zapewnić poprawność informacji wprowadzanych do systemu;
- d) Użytkownicy są zobowiązani do informowania o wszelkich nieprawidłowościach, zauważonych błędach w działaniu KSI SIMIK 07-13, zgodnie z dokumentem „Service Desk dla KSI SIMIK 07-13”.

2. Szkolenia użytkowników

- a) Użytkownicy KSI SIMIK 07-13, zobowiązani są do uczestnictwa w organizowanych szkoleniach w zakresie polityki bezpieczeństwa i procedur obowiązujących w tym zakresie;
- b) Użytkownicy KSI SIMIK 07-13, zobowiązani są do uczestnictwa także w innych szkoleniach, które doskonalą umiejętności pracy w systemie.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XI. Bezpieczeństwo fizyczne i środowiskowe głównej infrastruktury systemu

1. Dostęp do pomieszczenia, gdzie znajduje się główna infrastruktura jest możliwy tylko dla osób upoważnionych.
2. Dostęp do pomieszczenia i przebywanie w serwerowni dla nie zatrudnionych w MF możliwy jest tylko w uzasadnionych przypadkach, po podpisaniu oświadczeń o zachowaniu poufności i w obecności Administratorów Technicznych MF. Szczegółowe zasady w tym zakresie zdefiniowane są w dokumencie „Instrukcja zarządzania KSI SIMIK 07-13”. Po wykonaniu działań przez osoby z zewnątrz należy sporządzić odpowiedni protokół z przebiegu czynności
3. Drzwi do pomieszczenia serwerowni są zawsze zamykane oraz posiadają odpowiednie zamki i wytrzymałość co uniemożliwi łatwy dostęp do pomieszczenia.
4. W pomieszczeniu serwerowni nie wolno używać sprzętu fotograficznego, video, lub innych urządzeń do rejestracji informacji bez zgody AI lub ABI.
5. Pomieszczenie gdzie znajduje się główna infrastruktura KSI SIMIK 07-13, powinna uwzględniać minimalizację ryzyka wystąpienia potencjalnych zagrożeń, tj. kradzież, pożar, zalanie, promieniowanie elektromagnetyczne czy zanik zasilania.
6. W pomieszczeniu serwerowni obowiązuje całkowity zakaz jedzenia, picia i palenia tytoniu.
7. W pomieszczeniu serwerowni należy zapewnić urządzenia umożliwiające błyskawiczne gaszenie ewentualnego pożaru.
8. Sieć zasilająca w serwerowni musi być wydzielona, musi posiadać własne bezpieczniki przeciążeniowe.
9. Serwery systemu muszą posiadać urządzenia zapewniające podtrzymanie napięcia, tak aby zapewnić bezprzerwową pracę systemu.
10. W serwerowni musi znajdować się system zapewniający klimatyzację, dla urządzeń systemu.
11. W serwerowni nie mogą znajdować się materiały łatwopalne.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XII. Zarządzanie systemem i siecią dla głównej infrastruktury systemu

1. Zarządzanie serwerami

- a) Serwery KSI SIMIK 07-13, muszą być chronione przez oprogramowanie antywirusowe.
- b) Możliwość logowania się do serwerów systemu posiadają uprawnione osoby, w tym Administratorzy Techniczni MF.
- c) Administratorzy Techniczni zobowiązani są do zachowania szczególnej uwagi w trakcie prowadzenia prac w obrębie systemów operacyjnych serwerów KSI SIMIK 07-13.
- d) Wszelkie nośniki, dostarczane z zewnątrz, a użytkowane na serwerach należy przed ich użyciem bezwzględnie sprawdzić oprogramowaniem aktualnym antywirusowym.
- e) Należy dokonywać regularnych przeglądów logów systemu, jak również wykorzystania zasobów systemu.
- f) Wszelkie działania w zakresie administracji systemami należy odnotowywać w dzienniku pracy systemu, wzór dziennika stanowi załącznik 1, do niniejszego dokumentu.
- g) Urządzenia systemu należy konserwować, stosując się do wyznaczonych przez producentów lub dostawców sprzętu terminów konserwacji.
- h) W przypadku konieczności Kierownictwo Projektu zapewni zakupy sprzętu kompatybilnego z obecnie użytkowanym sprzętem.
- i) Sprzęt komputerowy musi być przetestowany i formalnie zaakceptowany przed przeniesieniem do środowiska produkcyjnego.
- j) Wycofywanie sprzętu i niszczenie nośników informacji odbywa się zgodnie z dokumentem „ Procedura postępowania z nośnikami informacji w przypadku likwidacji urządzeń komputerowych”.
- k) Należy bezwzględnie wykonywać regularne kopie bezpieczeństwa zarówno baz danych jak też systemów operacyjnych, tak aby było możliwe szybkie odtworzenie

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

systemu w przypadku awarii. Kopie danych oraz systemów operacyjnych należy przechowywać na odpowiednio trwałych nośnikach i odpowiednim sejfie, szczególne informacje na temat procesu wykonywania kopii bezpieczeństwa znajdują się w dokumencie „Procedura backupu KSI SIMIK 07-13”.

- l) Administratorzy Techniczni są zobowiązani do przeprowadzania regularnych przeglądów i aktualizacji systemów operacyjnych serwerów, baz danych, tzw. „hardening’u”.

2. Zarządzanie siecią

- a) Dostęp do konfiguracji urządzeń sieciowych odbywa się dopiero po podaniu prawidłowej nazwy użytkownika oraz hasła.
- b) Administratorzy Techniczni mają obowiązek zmiany domyślnych haseł i użytkowników dostarczonych wraz z domyślną konfiguracją urządzenia.
- c) Zarządzanie urządzeniami sieciowymi nie może być możliwe z dowolnej stacji roboczej, należy ściśle ograniczyć dostęp do konfiguracji urządzeń sieciowych do wydzielonych stacji roboczych.
- d) Konfiguracja i administracja urządzeniami sieciowymi wchodzącymi w skład głównej infrastruktury KSI SIMIK 07-13, wykonywana jest przez Administratorów Technicznych systemu w Ministerstwie Finansów oraz w części przez Departament Informatyki, Ministerstwa Finansów.
- e) Serwery KSI SIMIK 07-13, zlokalizowane są w chronionych segmentach sieci MF.
- f) Połączenia do Internetu realizowane są za pomocą dedykowanych łączy i urządzeń zapewniających ochronę systemu.
- g) Połączenie systemu z wewnętrzną siecią LAN w MF realizowane jest za pośrednictwem odpowiednich łączy i urządzeń zapewniających ochronę systemu.
- h) Aktywność urządzeń sieciowych jest rejestrowana w plikach logów oraz monitorowana przez Administratorów Technicznych.
- i) Kopie konfiguracji aktywnych urządzeń sieciowych są przechowywane na trwałych nośnikach w odpowiednich sejfach, szczególne informacje na temat procesu

| | | | |
|--|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

wykonywania kopii bezpieczeństwa znajdują się w dokumencie „Procedura backupu KSI SIMIK 07-13”.

- j) Administratorzy Techniczni są zobowiązani do dokonywania regularnej aktualizacji oprogramowania w urządzeniach aktywnych sieci.
- k) Wszystkie połączenia między siecią MF a siecią publiczną musi odbywać się przy użyciu odpowiednich urządzeń zapewniających bezpieczeństwo systemu.

Administratorzy Techniczni w MF muszą posiadać odpowiednią wiedzę techniczną z zakresu konfiguracji urządzeń sieciowych, serwerów i systemów operacyjnych tak aby zapewnić prawidłowe funkcjonowanie KSI SIMIK 07-13.

Administratorzy muszą podlegać okresowym szkoleniom z tego zakresu, aby ich stan wiedzy odpowiadał aktualnym rozwiązaniom i pojawiającym się zagrożeniom.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XIII. Kontrola dostępu

1. Dostęp użytkowników do systemu

- a) Tylko uprawnieni użytkownicy mogą uzyskać dostęp do KSI SIMIK 07-13.
- b) Dostęp do systemu musi być indywidualnie zdefiniowany dla każdego użytkownika. Użytkownik może mieć dostęp jedynie do zasobów, które są mu niezbędne do wykonywania obowiązków służbowych.
- c) Udzielanie, unieważnianie i ograniczanie dostępu użytkowników do systemu odbywa się w oparciu o zasady zdefiniowane w dokumencie „Procedura zgłaszania Użytkownika do Krajowego Systemu Informatycznego SIMIK 07-13 (nadawanie, zmiana, wygaśnięcie uprawnień) oraz zakres obowiązków administratorów merytorycznych”, opracowanym przez MRR.
- d) Nadanie lub zmiana uprawnień użytkownika następuje wyłącznie na wniosek sporządzony pisemnie, zgodnie z zasadami w dokumencie Procedura zgłaszania Użytkownika do Krajowego Systemu Informatycznego SIMIK 07-13 (nadawanie, zmiana, wygaśnięcie uprawnień) oraz zakres obowiązków administratorów merytorycznych”, opracowanym przez MRR.
- e) Tożsamość użytkowników jest sprawdzana po podaniu użytkownika i hasła do systemu, zalecenia co do bezpieczeństwa haseł opisuje dokument: „Zalecenia w sprawie bezpieczeństwa haseł Użytkowników”.
- f) Konto użytkownika musi być zablokowane po 30 dniach nieaktywności.
- g) Uprawnienia posiadane przez użytkowników nie mogą być rozszerzane, o ile nie istnieje umotywowana potrzeba związana ze zmianą zakresu obowiązków.

2. Polityka haseł

- a) Wszyscy użytkownicy muszą stosować hasła zgodne z zasadami ustalonymi w dokumencie „Zalecenia w sprawie bezpieczeństwa haseł użytkowników KSI SIMIK 07-13”.
- b) KSI SIMIK 07-13, umożliwia ustalenie minimalnej długości hasła, okresu

| | | | |
|--|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

maksymalnej ważności hasła oraz uniemożliwia powtórne wykorzystanie tego samego hasła.

- c) Haseł nie należy zapisywać i pozostawiać w miejscu w którym mogłyby zostać ujawnione.
- d) Hasła nie powinny być wpisywane w obecności osób trzecich, jeśli mogą one zauważyć treść wpisywanego hasła.
- e) Bez względu na okoliczności użytkownik nie może ujawniać swojego hasła do systemu, jakimkolwiek osobom.
- f) Jeśli istnieje podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić.
- g) Użytkownik ponosi pełną i absolutną odpowiedzialność za użycie zasobów systemu przy wykorzystaniu.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XIV. Monitorowanie bezpieczeństwa

1. System jest wyposażony w mechanizmy umożliwiające monitorowanie bezpieczeństwa, np. rejestrujące próby uzyskania dostępu do systemu.
2. Rejestry zdarzeń są regularnie przeglądane przez Administratorów Technicznych.
3. Każdy użytkownik systemu ma obowiązek zgłaszania zauważonych potencjalnych luk w zakresie bezpieczeństwa zgodnie z dokumentem „Service desk dla KSI SIMIK 07-13”.
4. ABI przygotowuje kwartalny raport z prowadzonego monitorowania i przekazuje go do AI.
5. AT monitoruje poprawność funkcjonowania systemu informatycznego oraz elementy systemu mające wpływ na bezpieczeństwo przetwarzanych informacji.
6. Ryzyka powinny być regularnie monitorowane przez ABI i AT. Przeglądy i aktualizacja dokumentu „Analiza ryzyka dla KSI SIMIK 07-13” należy przeprowadzać zgodnie z dokumentem „Zasady aktualizacji dokumentacji bezpieczeństwa KSI SIMIK 07-13”.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XV. Naruszenia bezpieczeństwa

1. Przypadki naruszenia bezpieczeństwa KSI SIMIK 07-13, powinny być natychmiast zgłaszane zgodnie z dokumentem „Service desk dla KSI SIMIK 07-13”.
2. W celu właściwego postępowania w przypadku naruszenia bezpieczeństwa systemu, należy gromadzić wszelkie informacje dotyczące skutków i charakteru tych przypadków.
3. Przypadki naruszenia bezpieczeństwa są analizowane przez ABI, zgodnie z procedurą w dokumencie „Service desk dla KSI SIMIK 07-13”.
4. Informacje o zgłoszonych przypadkach naruszenia bezpieczeństwa są ujmowane w kwartalnych raportach bezpieczeństwa KSI SIMIK 07-13.
5. W szczególnych przypadkach naruszenia bezpieczeństwa KSI SIMIK 07-13, powoływany jest Zespół Kryzysowy (ZK).

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XVI. Rozwój systemu

1. Narzędzia i programy służące do testowania nowych wersji oprogramowania mogą być używane wyłącznie przez upoważnione osoby dla celów testowych i rozwojowych. Dostęp do tych narzędzi jest ściśle kontrolowany.
2. Środowisko produkcyjne powinno być fizycznie odseparowane od środowisk testowego i programistycznego, poprzez ich lokalizację na oddzielnych serwerach.
3. Uprawnienia osób pracujących w środowiskach produkcyjnym, testowym i programistycznym muszą być zróżnicowane,
4. Testowanie nowych wersji aplikacji nie może być przeprowadzane przez osoby zajmujące się rozwojem oprogramowania.
5. Plan i zakres testów określają odrębne dokumenty.
6. Dostawca oprogramowania nie może być zaangażowany w bieżącą obsługę oprogramowania. Dostawca oprogramowania musi być zaangażowany w formalne testy wspólnie z użytkownikami systemu.
7. Zmiany w systemie KSI SIMIK 07-13, muszą być autoryzowane i wprowadzane w sposób bezpieczny, umożliwiający prawidłowe przetwarzanie danych oraz zapewniający powrót do poprzednich wersji.
8. W celu zapewnienia, że wykonywane zmiany są autoryzowane, należy postępować zgodnie z dokumentem „Service desk dla KSI SIMIK 07-13”.
9. Przebieg oraz wyniki testów muszą być udokumentowane.
10. Wszystkie instrukcje użytkownika i inne materiały przed przekazaniem użytkownikom wymagają zatwierdzenia przez AI.
11. System musi umożliwiać rejestrowanie następujących informacji:
 - a. Datę modyfikacji lub dodania rekordu;
 - b. Nazwę użytkownika modyfikującego lub wprowadzającego rekord;

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XVII. Zarządzanie ciągłością działania

1. Zasady postępowania i wszelkie informacje dla zapewnienia ciągłości działania KSI SIMIK 07-13, zawarte zostały w dokumencie „Plan ciągłości działania dla KSI SIMIK 07-13”.
2. Podstawowym wymogiem jest to aby KSI SIMIK 07-13, posiadał wszystkie istotne dla odtworzenia działania systemu kopie. Kopie mają zapewniać, że będzie możliwe odtworzenie danych i kontynuowanie działania systemu.
3. Zdefiniowany został dokument „Procedura backupu KSI SIMIK 07-13”, określający zasady postępowania w zakresie sporządzania, testowania i odtwarzania kopii bezpieczeństwa.
4. Kopie bezpieczeństwa muszą być wykonywane przed każdą aktualizacją aplikacji lub czynnością serwisową na infrastrukturze głównej KSI SIMIK 07-13.
5. ZBI przeprowadza okresowe testy odtwarzania danych o częstotliwości nie mniejszej niż raz na 6 miesięcy.
6. Do celów archiwizacji nie należy wykorzystywać nośników, które nie zapewniają wiarygodnego sposobu przechowywania informacji.
7. Ocena sytuacji jako awaryjnej dokonywana jest zgodnie z dokumentem „Plan ciągłości działania dla KSI SIMIK 07-13”.
8. Plany awaryjne powinny być okresowo testowane, tak jednakże aby nie zakłócić działania systemu.
9. Wszystkie zmiany w infrastrukturze głównej systemu, mogące mieć wpływ na jej funkcjonowanie w sytuacji awaryjnej, należy bezzwłocznie dokumentować i zmieniać zapisy w dokumencie „Plan ciągłości działania dla KSI SIMIK 07-13” i dokumentach z nim związanych.

| | | | |
|--|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XVIII. Szkolenia

1. Zasady szkolenia Użytkowników w zakresie bezpieczeństwa informacji opisane są w dokumencie „Opis szkoleń z bezpieczeństwa” (PBI-SZK).
2. Użytkownicy potwierdzają fakt zapoznania się z procedurami oraz zobowiązanie do ich realizacji własnoręcznym podpisem na wykazie przeszkolonych osób. Wykazy przechowywane są przez wyznaczoną osobę przez MRR. Na życzenie Instytucji wyznaczona osoba przez MRR przekazuje wykaz przeszkolonych osób dla danej Instytucji.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XIX. Słownik pojęć

Główna Infrastruktura – Urządzenia KSI SIMIK 07-13, tj. serwery systemu, urządzenia zasilające, oraz elementy aktywne sieci zlokalizowane w serwerowni systemu.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

XX. Załączniki

1. Załącznik 1. Wzór upoważnienia oraz zadania AT

| | |
|---|--|
| Upoważnienie osoby do pełnienia funkcji Administratora Technicznego (AT) KSI SIMIK 07-13 | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> upoważniam osobę: <div style="display: flex; justify-content: space-around; width: 100%;"> funkcja osoby uprawnionej do wydania upoważnienia </div> <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> do pełnienia funkcji AT zgodnie z zadaniami wymienionymi w dokumencie PBI-SIS w załączniku 1</p> <p style="text-align: right;">..... Podpis, DATA</p> | |
| <u>Oświadczenie AT</u> | |
| <p>Ja, niżej podpisany przyjmuję funkcję AT i zobowiązuję się do przestrzegania Polityki Bezpieczeństwa w zakresie nadanego mi upoważnienia.</p> <p style="text-align: right;">..... Podpis, DATA</p> | |

**wypełniać czytelnie, drukowanymi literami*

Zadania AT:

1. Zarządza (posiadając prawa administracyjne) następującymi urządzeniami należącymi do systemu:
 - a) urządzenia sieciowe, w szczególności: Firewall, akceleratory SSL, IPS,
 - b) serwery aplikacyjne i bazodanowe.
2. Zarządza (posiadając prawa administracyjne) następującymi programami (oprogramowaniem) należącymi do systemu:
 - a) systemy operacyjne i webowe serwerów aplikacyjnych,

| | | | |
|--|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

- b) systemy operacyjne serwerów bazodanych,
 - c) baza danych.
3. Bierze udział w pracach modernizacyjnych i rozwojowych systemu.
 4. Prowadzi dziennik pracy systemu na swoim stanowisku pracy. Wzór dziennika podano w załączniku 1 do niniejszego dokumentu.

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

2. Załącznik 2. Wzór upoważnienia oraz zadania AM IK NSRO

| | |
|--|--|
| <p>Upoważnienie osoby do pełnienia funkcji Administradora Merytorycznego IK NSRO (AM IK NSRO) KSI SIMIK 07-13</p> | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> upoważniam osobę: funkcja osoby uprawnionej do wydania upoważnienia <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> do pełnienia funkcji AM IK NSRO zgodnie z zadaniami wymienionymi w niniejszym upoważnieniu <div style="text-align: right;">Podpis, DATA</div> </p> | |
| <p><u>Oświadczenie AM IK NSRO</u></p> | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> przyjmuję funkcję AM IK NSRO. <div style="text-align: right;">Podpis, DATA</div> </p> | |

**wypełniać czytelnie, drukowanymi literami*

Zadania AM IK NSRO¹:

1. Administruje i zarządza uprawnieniami Użytkowników w ramach KSI SIMIK 07-13, w tym w szczególności nadaje hasła i loginy Użytkownikom, w zakresie określonym w „Procedurze zgłaszania Użytkownika do Krajowego Systemu Informatycznego SIMIK 07-13 (nadawanie, zmiana, wygaśnięcie uprawnień) oraz zakres obowiązków administratorów merytorycznych”.
2. Udziela odpowiedzi na pytania Użytkowników dotyczące zagadnień merytorycznych w zakresie wykorzystania KSI SIMIK 07-13.
3. Uczestniczy w pracach związanych z przygotowaniem założeń dla KSI SIMIK 07-13;
4. Prowadzi szkolenia z zakresu Polityki Bezpieczeństwa, archiwizuje oświadczenia przeszkolonych przez siebie Użytkowników.

¹ Niepotrzebne zadania skreślić

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

3. Załącznik 3. Wzór odwołania osoby z pełnienia funkcji AM IK NSRO

| | |
|---|--|
| Odwołanie osoby z pełnienia funkcji Administratora Merytorycznego IK NSRO (AM IK NSRO) KSI SIMIK 07-13 | |
| Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> odwołuję osobę: funkcja osoby uprawnionej do wydania upoważnienia <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> z pełnienia funkcji AM IK NSRO . <div style="text-align: right;"> Podpis, DATA </div> | |

**wypełniać czytelnie, drukowanymi literami*

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

4. Załącznik 4. Wzór upoważnienia oraz zadania AM IZ

| | |
|---|--|
| <p>Upoważnienie osoby do pełnienia funkcji Administradora Merytorycznego IZ (AM IZ) KSI SIMIK 07-13</p> | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> upoważniam osobę: funkcja osoby uprawnionej do wydania upoważnienia <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> do pełnienia funkcji AM IZ zgodnie z zadaniami wymienionymi w niniejszym upoważnieniu <div style="text-align: right;">Podpis, DATA</div> </p> | |
| <p><u>Oświadczenie AM IZ</u></p> | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> przyjmuję funkcję AM IZ. <div style="text-align: right;">Podpis, DATA</div> </p> | |

**wypełniać czytelnie, drukowanymi literami*

Zadania AM IZ²:

1. Administruje i zarządza uprawnieniami Użytkowników w ramach KSI SIMIK 07-13 w ramach danego programu operacyjnego, w zakresie określonym w „Procedurze zgłaszania Użytkownika do Krajowego Systemu Informatycznego SIMIK 07-13 (nadawanie, zmiana, wygaśnięcie uprawnień) oraz zakres obowiązków administratorów merytorycznych”.
2. Udziela odpowiedzi na pytania Użytkowników dotyczące zagadnień merytorycznych w ramach danego programu operacyjnego w zakresie wykorzystania KSI SIMIK 07-13;
3. Uczestniczy w pracach związanych z przygotowaniem założeń dla KSI SIMIK 07-13;

² Niepotrzebne zadania skreślić

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

4. Uczestniczy w organizacji szkoleń dotyczących wykorzystania KSI SIMIK 07-13 dla Użytkowników w ramach danego programu operacyjnego;
5. Prowadzi działania szkoleniowe dla Użytkowników KSI SIMIK 07-13 w ramach danego programu operacyjnego;
6. Współpracuje z Administratorem Merytorycznym w IK NSRO w sprawach związanych z wykorzystaniem KSI SIMIK 07-13;
7. Zarządza zmianami, tj. m.in. monitoruje zmiany prawne i proceduralne mające wpływ na dalszy rozwój systemu (np. zmiany przepisów prawa, procedur zarządzania i kontroli funduszy strukturalnych, zmiany organizacyjne, przesunięcia w tabelach finansowych programu operacyjnego) i rozwój funkcjonalny systemu pod względem administracyjnym (dostosowanie do zmieniających się przepisów i procedur).
8. Opracowuje i uaktualnia procedury związane z administrowaniem systemu.
9. Prowadzi szkolenia z zakresu Polityki Bezpieczeństwa, archiwizuje oświadczenia przeszkolonych przez siebie Użytkowników oraz przekazuje zestawienie przeszkolonych Użytkowników do AM IK NSRO odpowiedzialnego za gromadzenie informacji dot. przeszkolonych Użytkowników.

5. Załącznik 5. Wzór odwołania osoby z pełnienia funkcji AM IZ

| | |
|---|--|
| <p>Odwołanie osoby z pełnienia funkcji Administradora Merytorycznego IZ (AM IZ) KSI SIMIK 07-13</p> | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> <p>..... odwołuję osobę: funkcja osoby uprawnionej do wydania upoważnienia</p> <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> <p>z pełnienia funkcji AM IZ.</p> <p style="text-align: right;">..... Podpis, DATA</p> </p> | |

**wypełniać czytelnie, drukowanymi literami*

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

6. Załącznik 6. Wzór upoważnienia oraz zadania AM I w Instytucji

| | |
|---|--|
| <p>Upoważnienie osoby do pełnienia funkcji Administradora Merytorycznego w Instytucji (AM I) KSI SIMIK 07-13</p> | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> upoważniam osobę: funkcja osoby uprawnionej do wydania upoważnienia <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> do pełnienia funkcji AM I zgodnie z zadaniami wymienionymi w niniejszym upoważnieniu <div style="text-align: right;">..... Podpis, DATA</div> </p> | |
| <p><u>Oświadczenie AM I</u></p> | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> przyjmuję funkcję AM I. <div style="text-align: right;">..... Podpis, DATA</div> </p> | |

**wypełniać czytelnie, drukowanymi literami*

Zadania AM I³:

1. Identyfikuje i zarządza uprawnieniami Użytkowników w danej instytucji, w zakresie określonym w „Procedurze zgłaszania Użytkownika do Krajowego Systemu Informatycznego SIMIK 07-13 (nadawanie, zmiana, wygaśnięcie uprawnień) oraz zakres obowiązków administratorów merytorycznych”.
2. Udziela odpowiedzi na pytania Użytkowników dotyczące zagadnień merytorycznych w ramach danej instytucji w zakresie wykorzystania KSI SIMIK 07-13;
3. Współpracuje z Administratorem Merytorycznym IZ w sprawach związanych z wykorzystaniem KSI SIMIK 07-13.
4. Prowadzi szkolenia z zakresu Polityki Bezpieczeństwa, archiwizuje oświadczenia przeszkolonych przez siebie Użytkowników oraz przekazuje zestawienie przeszkolonych Użytkowników do AM IK NSRO odpowiedzialnego za gromadzenie informacji dot. przeszkolonych Użytkowników.

³ Niepotrzebne zadania skreślić

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

7. Załącznik 7. Wzór odwołania osoby z pełnienia funkcji **AM I**

| | |
|--|--|
| Odwołanie osoby z pełnienia funkcji Administratora Merytorycznego w Instytucji (AM I) KSI SIMIK 07-13 | |
| <p>Ja, niżej podpisany (a): <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> odwołuję osobę: funkcja osoby uprawnionej do wydania upoważnienia</p> <p>..... <div style="display: flex; justify-content: space-around; width: 100%;"> imię* nazwisko* </div> z pełnienia funkcji AM I.</p> <p style="text-align: right;">..... Podpis, DATA</p> | |

**wypełniać czytelnie, drukowanymi literami*

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

8. Załącznik 8. Raporty z monitorowania bezpieczeństwa IT

Wprowadza się obowiązek monitorowania następujących zdarzeń (co najmniej jedno z wymienionych poniżej) oraz raportowanie kwartalnie Radzie Projektu lub kierownikowi projektu KSI SIMIK 07-13 (ewentualnie z-cy kierownika projektu SIMIK 07-13) zgodnie z tabelą poniżej:

- incydenty naruszenia bezpieczeństwa sieciowego,
- elementy systemu nie posiadające odpowiednich zabezpieczeń,
- czas, jaki upłynął od momentu zgłoszenia usunięcia Użytkownika lub zmiany jego uprawnień do momentu wykonania tego w systemie,
- ilości Użytkowników, którzy wpisywali błędne loginy i hasła.

| | | |
|-------------------------------|-----------------------|--------------------------------------|
| Raport za okres: | | |
| Nazwa zdarzenia | Opis zdarzenia | Ilość zdarzeń w danym okresie |
| | | |

| | | | |
|---|------------|---|--------------------|
| Nazwa instytucji opracowującej dokument | | Ministerstwo Finansów/Ministerstwo Rozwoju Regionalnego | |
| Tytuł dokumentu | | Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13 | |
| Wersja dokumentu | 2.1 | Kod dokumentu | PBI-SIS-MF+MRR-2_1 |
| Data opracowania | 12.01.2009 | Kod zakresu dokumentu | KSI SIMIK 07-13 |

9. Załącznik 9. Wzór upoważnienia osoby do pełnienia funkcji ABI

| | |
|--|--|
| <p>Upoważnienie osoby do pełnienia funkcji Administradora Bezpieczeństwa Informacji (ABI) KSI SIMIK 07-13</p> | |
| <p>Ja, niżej podpisany (a): </p> <p style="text-align: center; margin-left: 100px;">imię*</p> <p style="text-align: center; margin-left: 300px;">nazwisko*</p> <p>jako upoważniam osobę:</p> <p style="text-align: center; margin-left: 100px;">funkcja osoby uprawnionej do wydania upoważnienia</p> <p>..... </p> <p style="text-align: center; margin-left: 100px;">imię*</p> <p style="text-align: center; margin-left: 300px;">nazwisko*</p> <p>do pełnienia funkcji ABI zgodnie z zadaniami wymienionymi w dokumentach PBI KSI SIMIK 07-13</p> <p style="text-align: right; margin-right: 50px;">..... Podpis, DATA</p> | |
| <p><u>Oświadczenie ABI</u></p> <p>Ja, niżej podpisany przyjmuję funkcję ABI i zobowiązuję się do przestrzegania Polityki Bezpieczeństwa w zakresie nadanego mi upoważnienia.</p> <p style="text-align: right; margin-right: 50px;">..... Podpis, DATA</p> | |

**wypełniać czytelnie, drukowanymi literami*

