

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

ZATWIERDZAM

.....
data *podpis, pieczęć*

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

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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	29.01.2009	Grzegorz Brandebura	Weryfikacja uwag wprowadzonych przez MRR.
3.0	15.02.2010	Andrzej Kuzawiński	Zastąpienie roli MF przez MRR po przeniesieniu Systemu, uwzględnienie roli Wykonawcy (ACPD)
3.1	15.11.2010	Łukasz Jastrzębski	Aktualizacja Dokumentu Głównego.
	15.03.2011	Andrzej Kuzawiński	Weryfikacja – wprowadzenie uwag
	11.04.2011	Andrzej Kuzawiński	Wprowadzenie uwag ZBI, definicji podatności i zmiana nazwy ABI na ABI KSI, AI na AI KSI

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

I. Spis treści

I.	Spis treści.....	3
II.	Wstęp.....	4
III.	Cel i zakres polityki bezpieczeństwa KSI SIMIK 07-13	5
IV.	Odwołania do innych dokumentów	6
V.	Opis i zasięg systemu.....	7
VI.	Zasoby KSI SIMIK 07-13.....	8
VII.	Obszary przetwarzania informacji	9
VIII.	Analiza ryzyka	10
VIII.	Hierarchia ról i zadań w KSI SIMIK 07-13.....	11
IX.	Organizacja bezpieczeństwa	14
X.	Bezpieczeństwo osobowe	16
1.	Zasady postępowania użytkowników	16
2.	Szkolenia użytkowników	16
XI.	Bezpieczeństwo fizyczne i środowiskowe głównej infrastruktury systemu	17
XII.	Zarządzanie systemem i siecią dla głównej infrastruktury systemu	18
1.	Zarządzanie serwerami	18
2.	Zarządzanie siecią.....	19
XIII.	Kontrola dostępu.....	21
XIV.	Monitorowanie bezpieczeństwa.....	23
XV.	Zagrożenia bezpieczeństwa	24
XVI.	Rozwój systemu.....	25
XVII.	Zarządzanie ciągłością działania.....	26
XVIII.	Szkolenia	27
XIX.	Słownik pojęć	28

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

II. Wstęp

Celem KSI SIMIK 07-13 jest gromadzenie i przekazywanie danych dotyczących wdrażania NSRO, a więc wsparcie procesu redystrybucji funduszy UE w perspektywie finansowania 2007 – 2013. Formułowanie zasad bezpieczeństwa 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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

III. Cel i zakres polityki bezpieczeństwa KSI SIMIK 07-13

Celem polityki bezpieczeństwa informacji dla KSI SIMIK 07-13 jest zdefiniowanie zasad, metod i środków ochrony informacji w systemie. Bezpieczeństwo informacji polega na zapewnieniu 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.

Niniejszą politykę stosuje się do wszystkich czynności związanych z gromadzeniem i przetwarzaniem informacji w KSI SIMIK 07-13 przez użytkowników i administratorów systemu, niezależnie od postanowień polityk i regulaminów obowiązujących w instytucjach użytkujących system. Polityki nie stosuje się do środowiska narzędziowego KSI SIMIK 07-13, utrzymywanego w MRR i podlegającego ochronie na podstawie „Polityki bezpieczeństwa systemów teleinformatycznych w Ministerstwie Rozwoju Regionalnego”.

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

IV. Odwołania do innych dokumentów

Na skutek zmiany zakresu PBI w związku z przeniesieniem infrastruktury teleinformatycznej Systemu do CPD ComArch S.A. następuje unieważnienie wszelkich dokumentów PBI o numerach wersji niższych niż 3.0. Dokumenty te otrzymują status wersji archiwalnych.

We wszystkich dokumentach o numerze wersji niższym niż 3.1 pod skrótem ABI należy rozumieć ABI KSI, natomiast pod skrótem AI należy rozumieć AI KSI.

Z niniejszym wydaniem PBI związane są następujące dokumenty:

1. Instrukcja postępowania ABI KSI w sytuacji zagrożenia bezpieczeństwa informacji KSI SIMIK 07-13 (PBI-INB-ABI)
2. Instrukcja postępowania ACPD w sytuacji zagrożenia bezpieczeństwa informacji KSI SIMIK 07-13 (PBI-INB-ACPD)
3. Instrukcja postępowania AM I w sytuacji zagrożenia bezpieczeństwa informacji KSI SIMIK 07-13 (PBI-INB-AM)
4. Instrukcja postępowania Użytkownika w sytuacji zagrożenia bezpieczeństwa informacji KSI SIMIK 07-13 oraz procedura powiadamiania AM przez Użytkownika w sytuacji zagrożenia bezpieczeństwa informacji (PBI-INB-USE)
5. Zalecenia dotyczące zabezpieczenia komputerów Użytkowników (PBI-INS)
6. Instrukcja zarządzania KSI SIMIK 07-13 (PBI-IZS)
7. Zalecenia w sprawie bezpieczeństwa haseł Użytkowników (PBI-PRC-UHS)
8. Procedura rozpoczynania, zawieszania i kończenia pracy w systemie przez Użytkownika (PBI-PRC-UAM)
9. Procedura przechowywania i udostępniania dokumentacji technicznej KSI SIMIK 07-13 (PBI-PRC-DOT)
10. Analiza Ryzyka dla KSI SIMIK 07-13 (PBI-AZR)
11. Spis zagrożeń dla Krajowego Systemu Informatycznego SIMIK 07-13 (PBI-SZA)
12. Zasady aktualizacji dokumentacji bezpieczeństwa KSI SIMIK 07-13 (PBI-ZAD)
13. Plan ciągłości działania KSI SIMIK 07-13 (PBI-PCD)
14. „Utrzymanie ciągłości pracy systemu KSI SIMIK 07-13 – Rozwiązania oraz Procedury”.
15. Zakresy zadań i dane kontaktowe ZK (PBI-TAB-ZKR)
16. Dane kontaktowe podmiotów zewnętrznych (PBI-WSP)
17. Wzory upoważnień i odwołań (PBI-UPO)
18. Procedura oznaczania i postępowania z informacją w KSI SIMIK 07-13 (PBI-OZN)

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

V. 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 Instytucji Koordynującej Narodowe Strategiczne Ramy Odniesienia – 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. MRR DI – Departament Informatyki MRR
- 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 dofinansowanymi przez Unię Europejską.

Powiązania KSI SIMIK 07-13 z innymi systemami:

- System SIMIK 2004-2006.
- System ISKOS, w zakresie kontroli środków pomocowych (5%, 15%).
- System PEFS.
- Systemy finansowo-księgowo poszczególnych instytucji.
- Lokalne Systemy Informatyczne, wykorzystywane przez poszczególne instytucje zaangażowane w proces zarządzania i kontroli wykorzystania funduszy UE.
- System SFC 2007).

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

VI. 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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

VII. 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 Centrum Przetwarzania Danych ComArch S.A, które znajduje się pod adresem: Al. Jana Pawła II 41 d, 31-864 Kraków, zapewniające zgodnie z Umową pracę i ochronę głównej infrastruktury systemu.
4. Środowiska narzędziowe (repozytoria wymagań, konfiguracji, zgłoszeń itp.) systemu jest utrzymywane w MRR i podlega ochronie na podstawie Polityki Bezpieczeństwa Informacji MRR.
5. Komunikacja z systemem odbywa się przy użyciu połączenia szyfrowanego (https), przy użyciu protokołu SSL.

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

VIII. 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” (PBI-AZR).

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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 Wykonawca wyłoniony w postępowaniu o udzielenie zamówienia publicznego.

MRR odpowiada m.in. za zarządzanie, nadawanie uprawnień wszystkim AM i Użytkownikom oraz za współpracę z Instytucjami korzystającymi z 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,. 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 KSI

Rolę Administratora Informacji KSI pełni z-ca dyrektora DI MRR, nadzorujący Wydział KSI SIMIK. Do zadań AI KSI należy:

- a) wyznaczenie osób pełniących rolę ABI KSI
- b) wyznaczenie osób pełniących rolę AT
- c) wyznaczenie członków ZBI
- d) powołanie w porozumieniu z Wykonawcą członków ZK
- e) analiza raportów otrzymywanych od ABI KSI
- f) powołanie dodatkowej komisji do przeprowadzenia postępowania wyjaśniającego w celu pełnego zbadania przyczyn i skutków incydentu,

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

ustalenia sprawcy oraz wielkości poniesionych strat

- g) określanie innych zadań związanych dotyczących Polityki Bezpieczeństwa i wyznaczenie do tych zadań osób.

2.2 ABI KSI

Administrator Bezpieczeństwa Informacji KSI to osoba lub zespół powołany przez AI KSI do zadań związanych z ochroną KSI SIMIK 07-13, w szczególności:

- a) reagowanie na incydenty zgodnie z „Instrukcją postępowania ABI w sytuacji zagrożenia 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 KSI.

2.3 AT

Administrator Techniczny - pracownik Departamentu Informatyki MRR, wyznaczony przez AI KSI do zarządzania KSI SIMIK 07-13 w zakresie:

- a) wsparcia w realizacji zmian w KSI SIMIK 07-13,
- b) obsługi zgłoszeń dotyczących problemów technicznych.

2.4 ACPD

Administrator Centrum Przetwarzania Danych - pracownik CPD ComArch S.A., wyznaczony do wykonywania czynności administratorskich i operatorskich w ramach świadczenia usługi Dedykowanego Hostingu Infrastruktury Teleinformatycznej KSI SIMIK 07-13.

2.5 AM IK NSRO

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

Administrator Merytoryczny IK NSRO - osoba wyznaczona przez MRR do zarządzania Użytkownikami (zakładanie/usuwanie kont Użytkowników, przyznawanie/odbieranie uprawnień Użytkowników).

2.6 AM IZ

Administrator Merytoryczny IZ - osoba wyznaczona przez Instytucję Zarządzającą do zarządzania Użytkownikami.

2.7 AM I

Administrator Merytoryczny w Instytucji - osoba wyznaczona przez Instytucję do zarządzania Użytkownikami.

Wzory upoważnień oraz szczegółowe zadania poszczególnych Administratorów określone są w dokumencie „Wzory upoważnień i odwołań (PBI-UPO)”.

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

IX. Organizacja bezpieczeństwa

1. Powołuje się **Administratorsa Bezpieczeństwa Informacji KSI (ABI KSI)** 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 zagrożenia bezpieczeństwa informacji”,
 - b) analiza i ewidencjonowanie zagrożeń,
 - 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 KSI.

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 Informacji KSI (AI KSI), Administrator Bezpieczeństwa Informacji KSI (ABI KSI), Administrator(rzy) Techniczni (AT), przedstawiciel(e) Wykonawcy, przedstawiciel(e) Głównego Użytkownika (IK NSRO).

3. Powołuje się **Zespół Kryzysowy (ZK)** w celu koordynacji oraz analizy działań podjętych przez Wykonawcę 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 spowodowałoby konsekwencje polityczne, medialne) KSI SIMIK 07-13. W skład zespołu powinni wchodzić następujące osoby:
 - Przedstawiciel(e) MRR,
 - Przedstawiciel(e) Wykonawcy,

Zespół może powołać na zasadzie ekspertów osoby ze stanowiska ds. ochrony informacji niejawnych MRR, osoby z biura prasowego MRR, osoby z departamentu prawnego MRR.

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

Członkowie ZK wybierają spośród siebie Koordynatora ZK oraz jego zastępcę, którzy pełnią funkcje organizacyjne związane z pracami ZK, np. przewodniczenie posiedzeniom, pisanie protokołów lub notatek z posiedzeń, informowanie pozostałych członków 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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

XI. Bezpieczeństwo fizyczne i środowiskowe głównej infrastruktury systemu

Zgodnie ze Szczegółowym Opiszem Przedmiotu Zamówienia, Wykonawca, w trakcie świadczenia usługi Dedykowanego Hostingu Infrastruktury Teleinformatycznej jest zobowiązany do zapewnienia bezpieczeństwa Systemu oraz przechowywanych informacji.

- a) Zagwarantowany poziom bezpieczeństwa powinien uniemożliwić dokonanie włamania, uzyskanie jakiegokolwiek nieautoryzowanego dostępu do systemu i danych oraz zakłócenia lub przerwania jego pracy;
- b) Zastosowane zabezpieczenia powinny co najmniej spełniać wymagania określone w Załączniku A do normy PN-ISO/IEC 27001:2007;
- c) Wykonywanie kopii bezpieczeństwa oprogramowania i baz danych powinno się odbywać w godzinach 24.00 – 6.00 w sposób umożliwiający ich poprawne odtworzenie.

Wykonawca ma obowiązek wykonywania niezbędnych czynności administracyjnych i operatorskich, mających na celu zapewnienie funkcjonowania, bezpieczeństwa oraz dostępności Oprogramowania.

Zabezpieczenia fizyczne infrastruktury Systemu, utrzymywanej w Centrum Przetwarzania Danych ComArch S.A. opisane są w dokumencie „Utrzymanie ciągłości pracy systemu KSI SIMIK 07-13 – Rozwiązania oraz Procedury”.

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

XII. Zarządzanie systemem i siecią dla głównej infrastruktury systemu

1. Zarządzanie serwerami

- a) Możliwość logowania się do serwerów systemu posiadają tylko uprawnione osoby.
- b) Administratorzy CPD ComArch S.A. (ACPD) zobowiązani są do zachowania szczególnej uwagi w trakcie prowadzenia prac w obrębie systemów operacyjnych serwerów KSI SIMIK 07-13.
- c) Wszelkie nośniki, dostarczane z zewnątrz, a użytkowane na serwerach należy przed ich użyciem bezwzględnie sprawdzić aktualnym oprogramowaniem antywirusowym.
- d) Należy dokonywać regularnych przeglądów logów systemu, jak również wykorzystania zasobów systemu.
- e) Wszelkie działania w zakresie administracji systemami należy odnotowywać w dzienniku pracy systemu,
- f) Urządzenia systemu należy konserwować, stosując się do wyznaczonych przez producentów lub dostawców sprzętu terminów konserwacji.
- g) Sprzęt komputerowy musi być przetestowany i formalnie zaakceptowany przed przeniesieniem do środowiska produkcyjnego.
- h) Wycofywanie sprzętu i niszczenie nośników informacji odbywa się zgodnie z zaleceniami zawartymi w „Polityce bezpieczeństwa MRR”.
- i) Należy bezwzględnie wykonywać regularne kopie bezpieczeństwa zarówno baz danych jak też systemów operacyjnych, tak aby było możliwe szybkie odtworzenie systemu w przypadku awarii. Kopie danych oraz systemów operacyjnych należy przechowywać na odpowiednio trwałych nośnikach i w odpowiednim sejfie. Szczegółowe informacje na temat procesu wykonywania kopii bezpieczeństwa znajdują się w dokumencie „Utrzymanie ciągłości pracy systemu KSI SIMIK 07-13 – Rozwiązania oraz Procedury”.
- j) Administratorzy CPD ComArch S.A. (ACPD) są zobowiązani do przeprowadzania regularnych przeglądów i aktualizacji systemów operacyjnych serwerów, baz danych,

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

tw. „hardening’u”.

2. Zarządzanie siecią

- a) Dostęp do konfiguracji urządzeń sieciowych odbywa się dopiero po podaniu prawidłowej nazwy użytkownika oraz hasła.
- b) Administratorzy CPD ComArch S.A. 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 ACPD.
- e) Serwery KSI SIMIK 07-13, zlokalizowane są w chronionych segmentach sieci Wykonawcy.
- f) Połączenia do Internetu realizowane są za pomocą dedykowanych łączy i urządzeń zapewniających ochronę systemu.
- g) Połączenie systemu z wewnętrzną siecią LAN Wykonawcy realizowane jest za pośrednictwem odpowiednich łączy i urządzeń zapewniających ochronę systemu.
- h) Aktywność urządzeń sieciowych jest rejestrowana w plikach logów oraz monitorowana przez ACPD.
- i) Kopie konfiguracji aktywnych urządzeń sieciowych są przechowywane na trwałych nośnikach w odpowiednich sejfach, szczegółowe informacje na temat procesu wykonywania kopii bezpieczeństwa znajdują się w dokumencie „Utrzymanie ciągłości pracy systemu KSI SIMIK 07-13 – Rozwiązania oraz Procedury”.
- j) ACPD są zobowiązani do dokonywania regularnej aktualizacji oprogramowania w urządzeniach aktywnych sieci.
- k) Wszystkie połączenia między siecią CPD ComArch S.A. a siecią publiczną musi odbywać się przy użyciu odpowiednich urządzeń zapewniających bezpieczeństwo systemu.

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

ACPD 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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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 posiadanego hasła.

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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 ACPD.
3. Każdy użytkownik systemu ma obowiązek zgłaszania zauważonych potencjalnych podatności (luk, słabości) w zakresie bezpieczeństwa zgodnie z dokumentem „Service Desk dla KSI SIMIK 07-13”.
4. ABI KSI monitoruje:
 - a) wystąpienia zagrożeń bezpieczeństwa (podatności, zdarzeń, incydentów),
 - b) czas, jaki upłynął od momentu zgłoszenia zablokowania Użytkownika lub zmiany jego uprawnień do chwili odnotowania tego w systemie,
 - c) ilość Użytkowników, którzy wpisywali błędne loginy i hasła.
5. ABI KSI przygotowuje kwartalny raport z prowadzonego monitorowania i przekazuje go do AI KSI.
6. Ryzyka powinny być regularnie monitorowane przez ABI KSI. 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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	Kod zakresu dokumentu	KSI SIMIK 07-13

XV. Zagrożenia bezpieczeństwa

1. Przypadkami wskazującymi na zagrożenie bezpieczeństwa informacji są:
 - a) **Podatność** (luka, słabość) aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako **potencjalna przyczyna** niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji
 - b) **Zdarzenie** związane z bezpieczeństwem informacji, które jest stanem systemu, usługi lub sieci, **wskazującym na możliwe naruszenie** polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
 - c) **Incydent** związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają **znaczne prawdopodobieństwo** zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
2. Podatności, zdarzenia i incydenty związane z bezpieczeństwem KSI SIMIK 07-13, powinny być natychmiast zgłaszane zgodnie z dokumentem „Service Desk dla KSI SIMIK 07-13”.
3. W celu właściwego postępowania w przypadku stwierdzenia zagrożenia bezpieczeństwa systemu, należy gromadzić wszelkie informacje dotyczące skutków i charakteru tych przypadków.
4. Przypadki zagrożenia bezpieczeństwa są analizowane przez ABI KSI, zgodnie z procedurą
Instrukcja postępowania ABI w sytuacji zagrożenia bezpieczeństwa informacji KSI SIMIK 07-13 (PBI-INB-ABI)
5. Informacje o zgłoszonych przypadkach zagrożenia bezpieczeństwa są ujmowane w kwartalnych raportach bezpieczeństwa KSI SIMIK 07-13 sporządzanych przez ABI KSI.
6. W szczególnych przypadkach naruszenia bezpieczeństwa KSI SIMIK 07-13, zwoływany jest Zespół Kryzysowy (ZK).

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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. 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.
7. W celu zapewnienia, że wykonywane zmiany są autoryzowane, należy postępować zgodnie z dokumentem „Service Desk dla KSI SIMIK 07-13”.
8. Przebieg oraz wyniki testów muszą być udokumentowane.
9. System musi umożliwiać rejestrowanie następujących informacji:
 - a) Datę modyfikacji lub dodania rekordu;
 - b) Nazwę użytkownika modyfikującego lub wprowadzającego rekord.

Nazwa instytucji opracowującej dokument		Ministerstwo Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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. Kopie bezpieczeństwa muszą być wykonywane przed każdą aktualizacją aplikacji lub czynnością serwisową przeprowadzaną w infrastrukturze głównej KSI SIMIK 07-13.
4. ZBI przeprowadza okresowe testy odtwarzania danych o częstotliwości nie mniejszej niż raz na 6 miesięcy.
5. Do celów archiwizacji nie należy wykorzystywać nośników, które nie zapewniają wiarygodnego sposobu przechowywania informacji.
6. Ocena sytuacji jako awaryjnej dokonywana jest zgodnie z dokumentem „Plan ciągłości działania dla KSI SIMIK 07-13”.
7. Plany awaryjne powinny być okresowo testowane, tak jednakże aby nie zakłócić działania systemu.
8. 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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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 Rozwoju Regionalnego	
Tytuł dokumentu		Dokument główny Polityka bezpieczeństwa Informacji dla Krajowego Systemu Informatycznego SIMIK 07-13	
Wersja dokumentu	3.1	Kod dokumentu	PBI-SIS-3_1
Data opracowania	11.04.2011	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 DPD ComArch S.A.

Wykonawca - ComArch S.A., z siedzibą w Krakowie przy al. Jana Pawła II nr 39 A, 31-864 Kraków, strona Umowy DI/BDG-II/POPT/663/09 na utrzymanie oraz rozwój Oprogramowania KSI SIMIK 07-13 wraz z hostingiem infrastruktury teleinformatycznej.