

Krajowy System Informatyczny SIMIK 07-13

Tymczasowe procedury zgłaszania problemów/zmian/incydentów dot. naruszenia bezpieczeństwa informacyjnego.

Zatwierdzam:

Wersja 1.2.

Warszawa, dnia 31 marca 2009 roku

.....
(podpis i pieczętka)

Historia zmian

Numer wersji	Data Zatwierdzenia	Autorzy	Opis zmian
1.0	15-02-2008	Pracownicy Wydziału III	Zatwierdzenie
1.1	25-07-2008	Pracownicy Wydziału III	Aktualizacja i Zatwierdzenie
1.2	05-02-2009	Pracownicy Wydziału III	Aktualizacja i Weryfikacja
1.2	31-03-2009	Zastępca Dyrektora MRR DKF	Zatwierdzenie

Wykaz skrótów i definicji

Skrót	Opis skrótu
ABI	Administrator Bezpieczeństwa Informacji
<i>Administrator merytoryczny</i>	osoba lub zespół osób wyznaczony przez AI do zadań związanych z ochroną systemu skrót odnoszący się do każdego Administratora Merytorycznego, tj. do Administratora Merytorycznego w IK NSRO, Administratora Merytorycznego w IZ, Administratora Merytorycznego w Instytucji Stanowi bezpośrednie wsparcie Użytkowników z danej Instytucji.
<i>Administrator merytoryczny w IK NSRO</i> AM IK NSRO	Administrator Merytoryczny w IK NSRO (AM IK NSRO) – pracownik IK NSRO: <ul style="list-style-type: none"> • monitoruje proces wdrażania KSI (SIMIK 07-13), • wspiera utrzymanie i rozwój KSI (SIMIK 07-13), • nadaje uprawnienia Użytkownikom systemu KSI (SIMIK 07-13). Stanowi bezpośrednie wsparcie Użytkowników z MRR IK NSRO.
<i>Administrator merytoryczny w IZ</i> AM IZ	Administrator Merytoryczny w IZ (AM IZ) – pracownik IZ programem operacyjnym: <ul style="list-style-type: none"> • monitoruje proces wdrażania KSI SIMIK 07-13 w instytucji zarządzającej, • monitoruje wprowadzanie danych do systemu przez pracowników w instytucji zarządzającej, • wspiera utrzymanie i rozwój KSI SIMIK 07-13; Stanowi bezpośrednie wsparcie Użytkowników z IZ. Uwaga: Instytucja Certyfikująca (IC) wyznacza również Administratora Merytorycznego. Pełni on rolę AM IZ dla wszystkich Instytucji Pośredniczących w Certyfikacji (IPOC).
<i>Administrator merytoryczny w instytucji</i> AM I	Administrator Merytoryczny w Instytucji (AM I) – pracownik Instytucji: <ul style="list-style-type: none"> • monitoruje proces wdrażania KSI SIMIK 07-13 w Instytucji, • monitoruje wprowadzanie danych do systemu przez pracowników Instytucji, • wspiera utrzymanie i rozwój KSI SIMIK 07-13. Stanowi bezpośrednie wsparcie Użytkowników Instytucji.
AI	Administrator Informacji
AT	Administrator Techniczny KSI SIMIK 07-13 - osoba z ramienia MF odpowiedzialna za obsługę zgłoszeń technicznych.
<i>Instytucja</i>	podmiot zaangażowany w proces wdrażania funduszy strukturalnych i Funduszu Spójności lub organ, dla którego dostęp do danych zgromadzonych w KSI (SIMIK 07-13) jest niezbędny do realizacji celów statutowych
IZ	Instytucja Zarządzająca programem operacyjnym.
IC	Instytucja Certyfikująca
IPOC	Instytucja Pośrednicząca w Certyfikacji
KSI SIMIK 07-13	Krajowy System Informatyczny SIMIK 07-13.
MF	Ministerstwo Finansów
MRR	Ministerstwo Rozwoju Regionalnego
<i>Problem merytoryczny</i>	wadliwe merytorycznie działanie KSI SIMIK 07-13 lub SIMIKXML lub Oracle Discoverer lub innej aplikacji, niezgodne z opisem wymagań określonych w dokumentacji dotyczącej KSI SIMIK 07-13, m.in. w instrukcjach użytkownika, wytycznych itd.
<i>Problem obsługowy</i>	problem związany z obsługą lub użytkowaniem KSI SIMIK 07-13 lub SIMIKXML lub Oracle Discoverer lub innej aplikacji
<i>Problem techniczny</i>	problem związany z: <ul style="list-style-type: none"> • nieprawidłowym technicznym działaniem KSI SIMIK 07-13 lub SIMIKXML lub Oracle Discoverer lub innej aplikacji lub • nieprawidłowym działaniem stacji roboczej użytkownika lub • nieprawidłowym działaniem sieci użytkownika lub inny problem nie będący problemem merytorycznym lub obsługowym
<i>Użytkownik</i>	osoba uprawniona do korzystania z systemu KSI (SIMIK 07-13), osoba wyznaczona przez instytucję do pracy z systemem KSI (SIMIK 07-13), także AM IK NSRO, AM IZ, AM I
<i>Wykonawca</i>	Jednostka, firma wykonująca zmiany w KSI SIMIK 07-13 na podstawie zgłoszeń zmian
<i>Zespół Analityczny w MRR</i>	Zespół Analityczny w Ministerstwie Rozwoju Regionalnego
<i>Zespół Projektowo-Techniczny MF</i>	Osoba/osoby z ramienia MF odpowiedzialne za: <ul style="list-style-type: none"> • wsparcie w realizacji zmian w KSI SIMIK 07-13, • wsparcie w rozwiązywaniu problemów merytorycznych w KSI SIMIK 07-13, • obsługę zgłoszeń dotyczących problemów technicznych lub naruszeń bezpieczeństwa
ZK	Zespół Kryzysowy
<i>Zmiana</i>	zmiana w KSI SIMIK 07-13 lub SIMIKXML spowodowana nowymi wymaganiami

I. Wstęp

Dokument przedstawia **propozycję działania i zorganizowania Service Desk do czasu wdrożenia narzędzia informatycznego Clear Quest na poziomie AM I (przeszkolenia AM I w zakresie obsługi ww. narzędzia).**

Niemniej każdy AM IZ (w zakresie swojego PO) może inaczej zorganizować obsługę zgłoszeń na poziomie AM I => AM IZ.

AM IZ zostali przeszkoleni w zakresie obsługi ww. narzędzia, w związku z czym zgłoszenia problemów kierowane do nich **można dokonywać wyłącznie za pomocą ww. narzędzia.**

II. Zgłoszenie problemu merytorycznego/obsługowego/zmiany

Schemat przepływu zgłoszeń w Service Desk został zamieszczony w załączniku do niniejszego dokumentu, tj.

- Zgłoszenie Problemu Merytorycznego, Obsługowego lub Technicznego przedstawiono w Załączniku nr 1 do niniejszego dokumentu
- Zgłoszenie Zmiany przedstawiono w Załączniku nr 2 do niniejszego dokumentu

Adresy e-mail AM I, AM IZ wraz z przydziałem do poszczególnych programów operacyjnych zamieszczone są na stronie MRR: <http://www.funduszeuropejskie.gov.pl/AnalizyRaportyPodsumowania/Strony/KSI.aspx>, Adres AM IK NSRO jest jeden: KSI.problemy@mrr.gov.pl. Użytkownicy zgłaszają problemy na adresy swoich właściwych Administratorów Merytorycznych.

III. Zgłoszenie incydentu dot. naruszenia bezpieczeństwa informacji

Definicja naruszenia bezpieczeństwa informacji

Przez naruszenie bezpieczeństwa informacji należy rozumieć wszelkie mogące mieć miejsce zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet, jeżeli nie prowadzą do wyżej wymienionych skutków. W szczególności są to wszelkie sytuacje, w których nastąpiła utrata (np. kradzież lub zniszczenie) lub nieuzasadniona modyfikacja danych lub części danych (nawet, jeśli możliwe jest całkowite odtworzenie utraconych danych) a także możliwość dostępu do danych dla osób nieupoważnionych.

Incydentem naruszenia bezpieczeństwa określa się każde określone zdarzenie lub działanie, naruszające bezpieczeństwo lub zasady ochrony informacji.

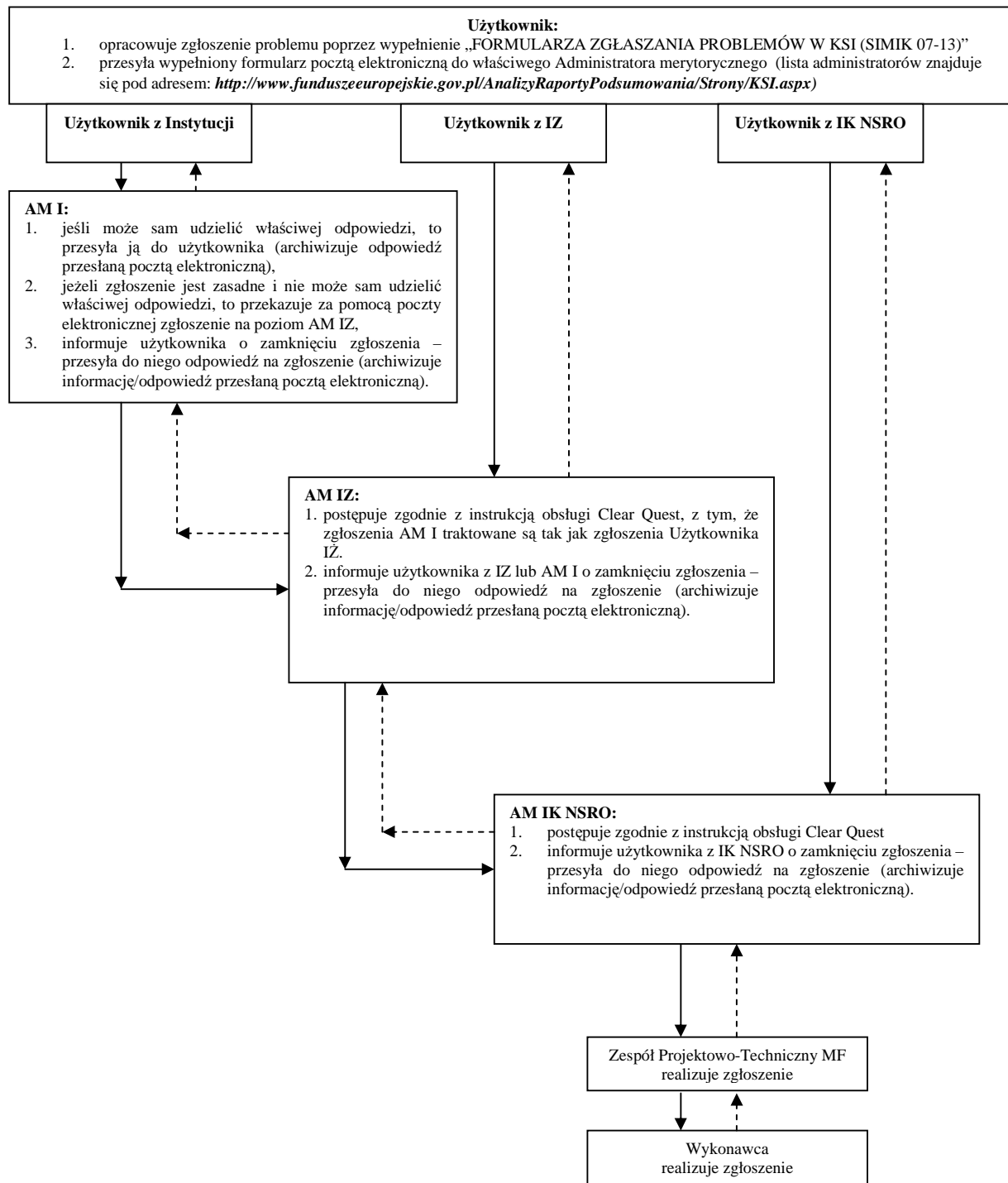
Na możliwość wystąpienia naruszenia bezpieczeństwa informacji mogą wskazywać:

- Nietypowy stan pomieszczeń przetwarzania (naruszone plomby, otwarte pomieszczenia, okna, drzwi od szaf, biurka, włączone urządzenia);
- Zaginięcie sprzętu lub nośników informacji (dyskietek, dokumentów papierowych, itp.);
- Nieuzasadnione modyfikacje lub usunięcie danych, niezgodności w danych;
- Nieprawidłowe lub nietypowe działanie systemu informatycznego (lub nietypowe komunikaty wyświetlane na monitorze).

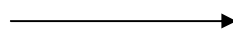
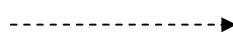
Schemat przepływu zgłoszeń w Service Desk został zamieszczony w załączniku 3 do niniejszego dokumentu

Adresy e-mail AM I, AM IZ wraz z przydziałem do poszczególnych programów operacyjnych zamieszczone są na stronie MRR: <http://www.funduszeuropejskie.gov.pl/AnalizyRaportyPodsumowania/Strony/KSI.aspx>, Adres AM IK NSRO jest jeden: KSI.incydenty@mrr.gov.pl

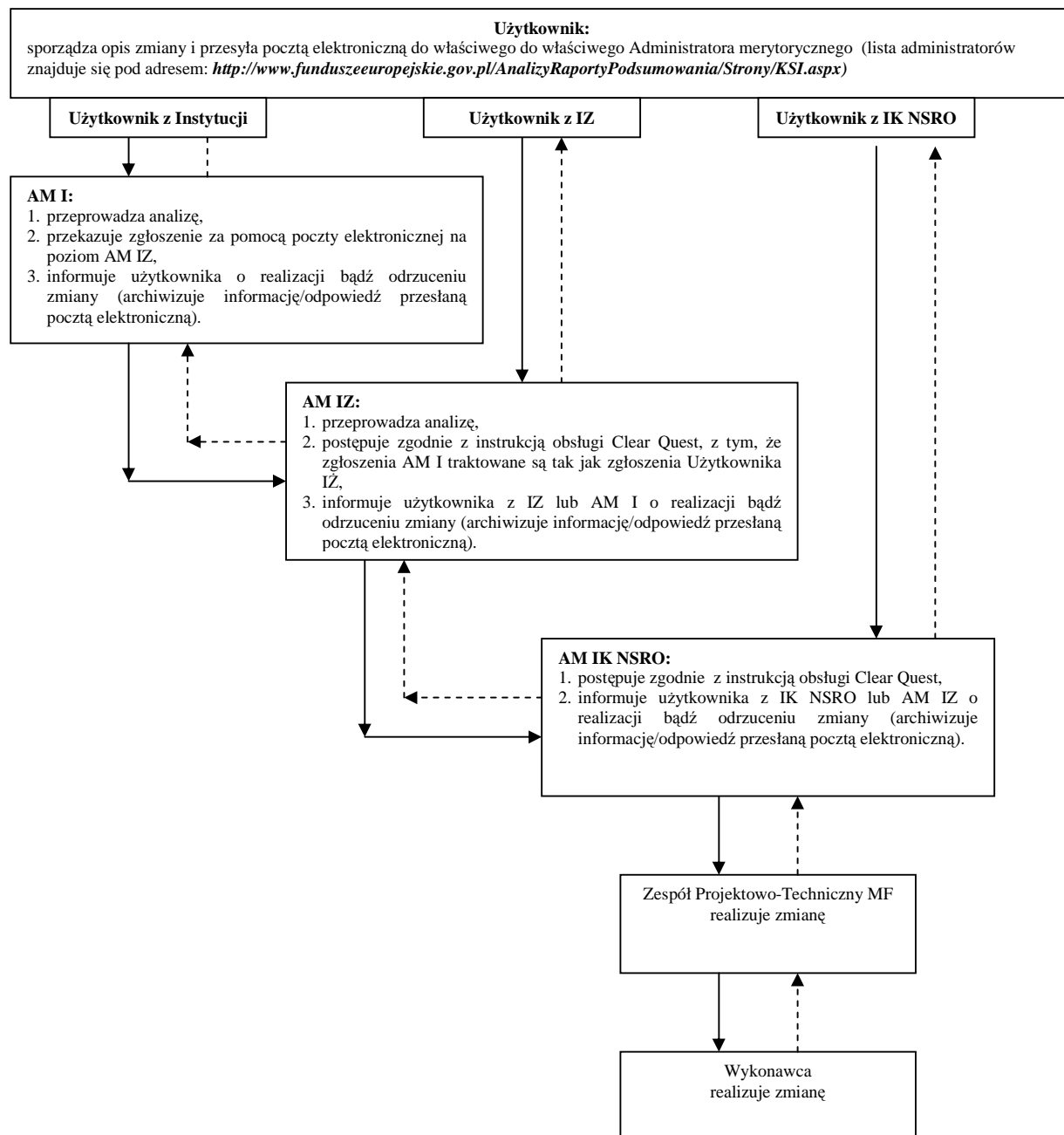
Załącznik 1. Zgłoszenie Problemu Merytorycznego, Obsługowego lub Technicznego



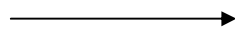
Legenda:

-  - zgłoszenie problemu
 - informacja zwrotna

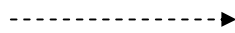
Załącznik 2. Zgłoszenie Zmiany



Legenda:



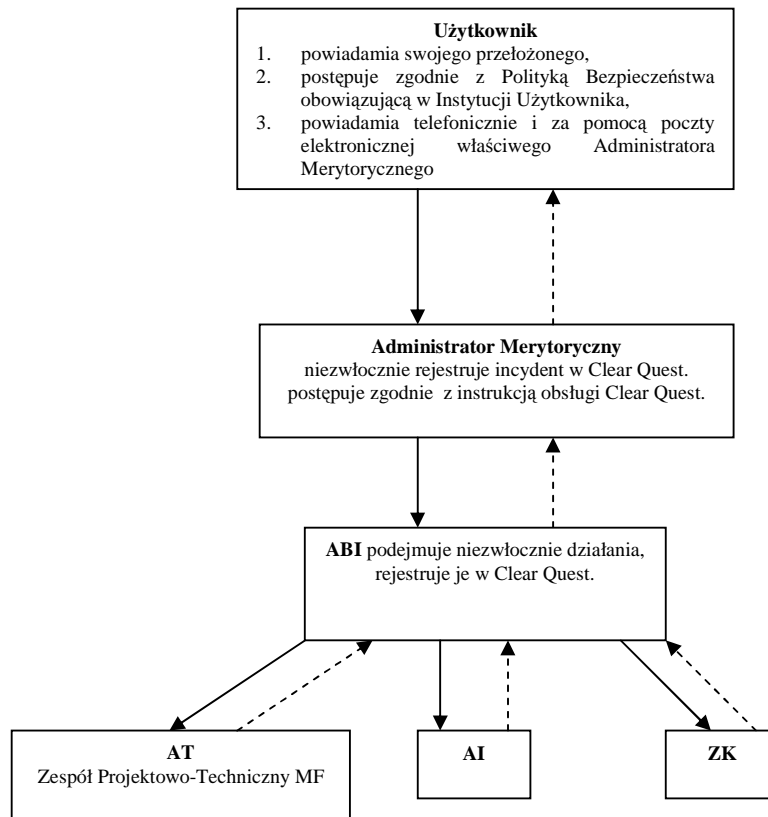
- zgłoszenie zmiany



- informacja zwrotna

Załącznik 3. Zgłoszenie incydentu

POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA INFORMACJI



Legenda:

- > - zgłoszenie
- - - - -> - informacja zwrotna