

PROCEDURA ZGŁASZANIA ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACJI PRZETWARZANYCH W CENTRALNYM SYSTEMIE TELEINFORMATYCZNYM	Wydanie nr 1
	Data: XX.XX.2016
	Strona 1 z 2

I. CEL PROCEDURY

Określenie sposobu postępowania w przypadku wystąpienia podatności, zdarzenia związanego z bezpieczeństwem informacji lub incydentu (w tym podatności, zdarzenia związanego z bezpieczeństwem informacji lub incydentu związanego z przetwarzaniem danych osobowych).

II. ZAKRES STOSOWANIA PROCEDURY

Procedura dotyczy wszystkich użytkowników centralnego systemu teleinformatycznego (w tym Użytkowników IW, Użytkowników B oraz K/Centrum FEDE).

III. PODSTAWA PRAWNA PROCEDURY

1. Zakres odpowiedzialności za bezpieczeństwo informacji przetwarzanych w centralnym systemie teleinformatycznym oraz szczegółowe zasady postępowania w przypadku naruszenia polityki bezpieczeństwa regulują dokumenty IZ/IK:

- Regulaminu bezpieczeństwa informacji przetwarzanych w centralnym systemie teleinformatycznym,

- Procedura obsługi zgłoszeń w Service Desk centralnego systemu teleinformatycznego.

2. Zakres odpowiedzialności za bezpieczeństwo informatyczne INiG-PIB oraz szczegółowe zasady postępowania w przypadku naruszenia polityki bezpieczeństwa regulują dokumenty wewnętrzne INiG-PIB:

- *Zarządzanie bezpieczeństwem informatycznym* – MP-01/PR-05,

- *Bezpieczeństwo przetwarzania danych osobowych* – MP-01/PR-05/IN-01,

- *Postępowanie w sytuacji naruszenia danych osobowych* – MP-01/PR-05/IN-03.

IV. SŁOWNIK

- 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;

- zdarzenie związane z bezpieczeństwem informacji – stan Systemu, usługi lub sieci, wskazujący na możliwe naruszenie Regulaminu, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;

- incydent – pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania Systemu i zagrażają bezpieczeństwu informacji, w tym danych osobowych przetwarzanych w Systemie;

- Użytkownik IW – osoba zatrudniona w IW mająca dostęp do SL2014 lub SL2014 wraz z SRHD;

- Użytkownik B – osoba uprawniona przez beneficjenta i mająca dostęp do SL2014;

- Administrator Techniczny odpowiadający za bezpieczeństwo centralnego systemu teleinformatycznego, ATB – wyznaczony pracownik Ministerstwa, który obsługuje zgłoszenia związane z bezpieczeństwem informacji przetwarzanych w Systemie;
- AM IW/Centrum FEDE - Administrator merytoryczny Instytucji Wdrażającej Centrum FEDE;
- K/Centrum FEDE - Kierownik Centrum FEDE.

V. OPIS PROCEDURY

1. Użytkownicy (w tym Użytkownicy IW i B) są zobowiązani do niezwłocznego powiadomienia (za pomocą poczty elektronicznej na adres: Centrum@inig.pl) AM IW/Centrum FEDE o podatności, zdarzeniu związanym z bezpieczeństwem informacji lub incydencie (w tym o podatności, zdarzeniu lub incydencie związanym z przetwarzaniem danych osobowych).
2. Użytkownicy wymienieni w pkt. 1. są zobowiązani do:
 - powstrzymywania się od wszelkich czynności mogących zatrzeć ślady naruszenia bezpieczeństwa informacji, w szczególności powstrzymywania się od wszelkich działań w systemie, zwłaszcza od usuwania podejrzanego oprogramowania,
 - stosowania się do poleceń AM IW/Centrum FEDE, o ile nie są one niezgodne z Polityką Bezpieczeństwa obowiązującą w Instytucji Użytkownika,
 - sporządzenia, wspólnie z Administratorem Merytorycznym IW, notatki o zagrożeniu, jeśli zostali o to poproszeni przez ATB.
3. AM IW/Centrum FEDE, postępując zgodnie z Procedurą obsługi zgłoszeń w Service Desk Centralnego Systemu Teleinformatycznego - pkt 3.3. Po otrzymaniu zgłoszenia podatności, zdarzenia lub incydentu dotyczącego bezpieczeństwa informacji (w tym podatności, zdarzenia lub incydentu związanego z przetwarzaniem danych osobowych), przeprowadza weryfikację zgłoszenia, rejestruje je w systemie Service Desk i postępuje zgodnie z zaleceniami IZ. Jednocześnie informuje K/Centrum FEDE i podejmuje działania zgodne z polityką bezpieczeństwa INiG-PIB. W przypadku braku dostępności systemu Service Desk dokonuje zgłoszenia pocztą elektroniczną na adres: cst.incydenty@mr.gov.pl.
4. AM IW/Centrum FEDE – w porozumieniu z Instytucjami wymienionymi w Procedurze obsługi zgłoszeń w Service Desk Centralnego Systemu Teleinformatycznego informuje zgłaszającego Użytkownika oraz jego służby informatyczne o sposobie dalszego postępowania, w tym, przesyła do w/w odpowiedź na zgłoszenie (archiwizuje informację/odpowiedź przestaną pocztą elektroniczną). Sporządza notatkę o zagrożeniu, jeśli zostali o to poproszeni przez ATB i stosuje się do zaleceń wydanych przez ATB.
5. Służby informatyczne Instytucji Użytkownika, po otrzymaniu zgłoszenia dotyczącego zagrożenia bezpieczeństwa informacji od AM IW/Centrum FEDE są zobowiązane do podjęcia działań i udzielania odpowiedzi.