



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
DLA SYSTEMU PODSYSTEM MONITOROWANIA
EUROPEJSKIEGO FUNDUSZ SPOŁECZNEGO 2007
U BENEFICJENTA PO KL**

Rozdział 1

Postanowienia ogólne

§ 1.

Instrukcja Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL, zwana dalej „Instrukcją”, określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w systemie Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007, zwanym dalej „PEFS 2007”, w
.....
zwany/ej dalej „Beneficjentem”.

§ 2.

Użyte w Instrukcji określenia oznaczają:

- | | |
|--|--|
| 1) Administrator Danych | - Ministra Rozwoju Regionalnego; |
| 2) użytkownik | - osobę upoważnioną, przez osobę upoważnioną do tego przez Administratora Danych, do przetwarzania danych osobowych w PEFS 2007; |
| 3) Administrator Bezpieczeństwa Informacji w IP/IP2 | - osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu IP/IP2, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 w IP/IP2; |
| 4) Administrator Bezpieczeństwa Informacji u Beneficjenta | - osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 u Beneficjenta; |
| 5) naruszenie zabezpieczenia PEFS 2007 | - jakiegokolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności PEFS 2007. |

Rozdział 2

Przydział haseł i identyfikatorów

§ 3.

Dla każdego użytkownika jest ustalany odrębny identyfikator i hasło dostępu do PEFS 2007.

§ 4.

Identyfikator użytkownika:

- 1) jest niepowtarzalny, a po wyrejestrowaniu użytkownika z PEFS 2007 nie jest przydzielany innej osobie;
- 2) jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, zgodnie z § 9, wraz z imieniem i nazwiskiem użytkownika.

§ 5.

Hasło użytkownika:

- 1) jest przydzielane indywidualnie dla każdego z użytkowników;
- 2) nie jest zapisane w systemie komputerowym w postaci jawnej;
- 3) jest zmieniane co najmniej raz na miesiąc;
- 4) powinno być utrzymywane w tajemnicy, również po upływie ważności.

§ 6.

Osobą odpowiedzialną za przydział identyfikatorów i pierwszych haseł dla użytkowników u Beneficjenta jest Administrator Bezpieczeństwa Informacji u Beneficjenta.

§ 7.

Przydziału i zmiany haseł dokonuje się w następujący sposób:

- 1) hasła powinny mieć co najmniej osiem znaków i muszą zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
- 2) hasło jest zmieniane przez każdego z użytkowników co najmniej raz na miesiąc;
- 3) hasła nie powinny składać się z kombinacji znaków mogących ułatwić ich odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko użytkownika);
- 4) hasło powinno zostać zmienione przez użytkownika niezwłocznie w przypadku powzięcia podejrzenia lub stwierdzenia, że mogły się z nim zapoznać osoby trzecie.

§ 8.

1. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora, który został mu przyznany.
2. Użytkownik jest zobowiązany utrzymywać hasło, którym się posługuje lub posługiwał, w ścisłej tajemnicy, w szczególności dołożyć wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem, nawet po ustaniu jego ważności.

Rozdział 3

Rejestrowanie i wyrejestrowywanie użytkowników

§ 9.

1. Rejestracji i wyrejestrowywania użytkowników dokonuje Administrator Bezpieczeństwa Informacji w u Beneficjenta.
2. Administrator Bezpieczeństwa Informacji u Beneficjenta prowadzi rejestr użytkowników, którego wzór został określony w załączniku nr 1 do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta.
3. Jakakolwiek zmiana informacji ujawnionych w rejestrze podlega natychmiastowemu

odnotowaniu i uaktualnieniu.

§ 10.

W PEFS 2007 może zostać zarejestrowany jedynie użytkownik, któremu osoba upoważniona przez Administratora Danych wydała upoważnienie do przetwarzania danych osobowych w PEFS 2007.

§ 11.

1. Z chwilą zarejestrowania w PEFS 2007 użytkownik jest informowany przez Administratora Bezpieczeństwa Informacji u Beneficjenta o ustalonym dla niego identyfikatorze i konieczności posługiwania się hasłami.
2. Administrator Bezpieczeństwa Informacji u Beneficjenta zapoznaje każdego nowego użytkownika z Instrukcją oraz Polityką Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta, a także z przepisami dotyczącymi ochrony danych osobowych, co użytkownik potwierdza swoim podpisem na liście, której wzór jest określony w załączniku nr 5 do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta.

§ 12.

Użytkownik jest wyrejestrowywany z PEFS 2007 w każdym przypadku utraty przez niego uprawnień do przetwarzania danych osobowych w PEFS 2007, co ma miejsce szczególnie w przypadku:

- 1) ustania zatrudnienia tego użytkownika u Beneficjenta lub zakończeniu przez tego użytkownika współpracy z Beneficjentem na podstawie umowy cywilno-prawnej;
- 2) zmiany zakresu obowiązków użytkownika powodujących utratę uprawnień do przetwarzania danych osobowych w PEFS 2007.

Rozdział 4

Rozpoczęcie, zawieszenie i zakończenie pracy w PEFS 2007

§ 13.

Użytkownik rozpoczynając pracę jest zobowiązany zalogować się do PEFS 2007 posługując się swoim identyfikatorem i hasłem.

§ 14.

1. W przypadku, gdy użytkownik planuje przerwać pracę, jest zobowiązany do zabezpieczenia dostępu do komputera za pomocą wygaszacza ekranu z aktywnym hasłem.
2. W przypadku, gdy użytkownik planuje przerwać pracę na dłuższy okres, a także kończąc pracę, jest zobowiązany wylogować się z PEFS 2007 oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki zawierające dane osobowe.

§ 15.

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczenia PEFS 2007 lub zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w PEFS 2007, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych w PEFS 2007, użytkownik jest zobowiązany niezwłocznie poinformować o tym Administratora Bezpieczeństwa Informacji u Beneficjenta, który jest

- zobowiązany poinformować o tym Administratora Bezpieczeństwa Informacji w IP/IP2.
2. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na okoliczności, o których mowa w ust. 1.

Rozdział 5

Tworzenie oraz przechowywanie kopii awaryjnych

§ 16.

Za tworzenie i przechowywanie u Beneficjenta kopii awaryjnych danych osobowych przetwarzanych w PEFS 2007 w sposób zgodny z przepisami prawa oraz poniższymi procedurami jest odpowiedzialny Administrator Bezpieczeństwa Informacji u Beneficjenta.

§ 17.

1. Kopie awaryjne danych osobowych przetwarzanych w PEFS 2007 są tworzone nie rzadziej niż raz na kwartał i zawierają pełny obraz zabezpieczanych danych osobowych znajdujących się na stacjach roboczych u Beneficjenta.
2. Kopie przechowuje się w różnych miejscach, w tym w lokalizacjach innych niż zbiór danych osobowych eksploatowany na bieżąco, w szczególności w odpowiednio zabezpieczonym pomieszczeniu znajdującym się w siedzibie Beneficjenta.

§ 18.

1. Kopie awaryjne danych osobowych przetwarzanych w PEFS 2007 po ustaniu ich użyteczności są bezzwłocznie usuwane.
2. Kopie awaryjne danych osobowych przetwarzanych w PEFS 2007, które uległy uszkodzeniu, podlegają natychmiastowemu zniszczeniu.

Rozdział 6

Ochrona PEFS 2007 przed wrogim oprogramowaniem

§ 19.

Bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych oraz koni trojańskich odbywa się przy zastosowaniu zainstalowanego na każdej stacji roboczej na bieżąco aktualizowanego programu antywirusowego, automatycznie monitorującego występowanie wirusów i koni trojańskich podczas operacji na plikach.

§ 20.

Nadzór nad instalowaniem oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Administrator Bezpieczeństwa Informacji u Beneficjenta.

§ 21.

O każdorazowym wykryciu wirusa lub konia trojańskiego przez oprogramowanie monitorujące użytkownik jest zobowiązany niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji u Beneficjenta; po usunięciu wirusa Administrator Bezpieczeństwa Informacji u Beneficjenta sprawdza PEFS 2007 oraz przywraca go do pełnej funkcjonalności i sprawności.

§ 22.

W ramach ochrony przed wrogim oprogramowaniem Administrator Bezpieczeństwa

Informacji u Beneficjenta stosuje logiczne i/lub fizyczne urządzenia firewall.

§ 23.

Żadne nośniki informacji zawierające dane osobowe nie są udostępniane poza obszar, w którym są przetwarzane dane osobowe.

Rozdział 7

Przeglądy i konserwacja PEFS 2007, sprzętu komputerowego oraz zbioru danych osobowych

§ 24.

Przeglądy i konserwacje sprzętu komputerowego wynikające ze zużycia sprzętu oraz warunków zewnętrznych i eksploatacji, z uwzględnieniem ważności sprzętu dla funkcjonowania PEFS 2007, są dokonywane przez Administratora Bezpieczeństwa Informacji u Beneficjenta.

§ 25.

Dyski lub inne informatyczne nośniki informacji umieszczone w urządzeniach przeznaczonych do napraw, gdzie jest wymagane zaangażowanie zewnętrznych firm serwisowych, usuwa się z tych urządzeń lub pozbawia się przed naprawą zapisu danych osobowych przetwarzanych w PEFS 2007. W przypadku niemożności usunięcia nośnika lub pozbawienia go zapisu tych danych osobowych naprawy dokonuje się pod nadzorem Administratora Bezpieczeństwa Informacji u Beneficjenta.

§ 26.

1. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przetwarzane w PEFS 2007, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przetwarzane w PEFS 2007, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych osobowych, pozbawia się wcześniej ich zapisu.

Rozdział 8

Postępowanie w zakresie komunikacji w sieci komputerowej

§ 27.

1. Dostęp do danych osobowych przetwarzanych w PEFS 2007 jest dozwolony jedynie po właściwym zalogowaniu się i podaniu własnego hasła użytkownika.
2. Wprowadzanie do PEFS 2007 informacji z zewnątrz, w szczególności danych osobowych, jest dopuszczalne tylko po stwierdzeniu legalności i wiarygodności źródeł informacji.

Rozdział 9

Wymagania sprzętowo-organizacyjne

§ 28.

Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.

§ 29.

Osoby nieuprawnione do dostępu do danych osobowych w PEFS 2007 mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe w PEFS 2007 wyłącznie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 30.

Decyzję o instalacji na stacji roboczej obsługującej przetwarzanie danych osobowych w PEFS 2007 jakiegokolwiek oprogramowania systemowego lub użytkowego podejmuje Administrator Bezpieczeństwa Informacji u Beneficjenta.

Rozdział 10 Postanowienia końcowe

§ 31.

Do spraw nieuregulowanych w Instrukcji stosuje się przepisy o ochronie danych osobowych.

§ 32.

Instrukcja nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia PEFS 2007.

