



ZARZĄDZENIE NR 201/13
Wójta Gminy Suwałki
z dnia 22 lipca 2013 roku

w sprawie wprowadzenia instrukcji zarządzania systemem informatycznym oraz Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki w ramach realizacji projektów współfinansowanych ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego .

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz.U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271, z 2004 r. Nr 25, poz.219 i Nr 33, poz. 285 z 2006 r. Nr 104, poz.708 i Nr 104, poz. 711, z 2007 r. Nr 165, poz.1170 i Nr 176, poz. 1238 oraz z 2010 r. Nr 41, poz. 233 oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzani danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024) zarządzam , co następuje:

§ 1. Wprowadzam instrukcję zarządzania systemem informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki, która stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2. Wprowadzam Politykę Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki, która stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 3. Wyznaczam do wykonywania obowiązków Administratora Bezpieczeństwa Informacji PEFS 2007 w Gminie Suwałki Pana Marka Lewczuka.

§ 4. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji PEFS 2007 w Gminie Suwałki.

§ 5. Zarządzenie wchodzi w życie z dniem podjęcia z mocą obowiązującą od dnia 1 sierpnia 2013 roku.



**załącznik nr 1
do zarządzenia nr 201/13
Wójta Gminy Suwałki
z dnia 22 lipca 2013 roku**

Instrukcja zarządzania systemem informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki.

Rozdział 1 Postanowienia ogólne

§ 1.

Instrukcja Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki, zwana dalej „Instrukcją”, określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w systemie Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki.

§ 2.

Użyte w Instrukcji określenia oznaczają:

1) Administrator Danych

- Instytucję Zarządzającą PO KL, oznacza to Departament Zarządzania Europejskim Funduszem Społecznym w Ministerstwie Rozwoju Regionalnego;

2) użytkownik

- osobę upoważnioną do przetwarzania danych osobowych w PEFS 2007;

3) Administrator Bezpieczeństwa Informacji PEFS 2007 w IP/IP2

- osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 we właściwej Instytucji Pośredniczącej /Instytucji Pośredniczącej II Stopnia PO KL;

4) Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta

- osobę odpowiedzialną za sprawność, konserwację, wdrażanie technicznych zabezpieczeń PEFS 2007 oraz nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 u Beneficjenta;



- 5) PEFS 2007** - podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL
- 6) PO KL** - Program Operacyjny Kapitał Ludzki
- 7) Beneficjent** - Gmina Suwałki
- 8) naruszenie zabezpieczenia PEFS 2007** - jakiegokolwiek zdarzenie lub działanie, które może stanowić przyczynę utraty zasobów, 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.

§ 6.

Osobą odpowiedzialną za przydział identyfikatorów i pierwszych haseł dla użytkowników jest Administrator Bezpieczeństwa Informacji PEFS 2007 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) hasła nie powinny składać się z kombinacji znaków mogących ułatwić ich odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko użytkownika);
- 3) hasło powinno zostać zmienione 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 PEFS 2007 u Beneficjenta.
2. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta prowadzi rejestr użytkowników, który stanowi załącznik nr 1 do Polityki Bezpieczeństwa dla zbioru 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 do tego osoba wydała upoważnienie do przetwarzania danych osobowych w PEFS 2007.

§ 11.

1. Po zarejestrowaniu w PEFS 2007 użytkownik jest informowany przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta o ustalonym dla niego identyfikatorze i konieczności posługiwania się hasłami.
2. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta jest odpowiedzialny za zapoznanie każdego nowego użytkownika z Instrukcją oraz Polityką Bezpieczeństwa dla zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta, a także z przepisami dotyczącymi ochrony danych osobowych, co użytkownik potwierdza swoim podpisem na liście, stanowiącej załącznik nr 3 do Polityki Bezpieczeństwa dla zbioru 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 PEFS 2007 u Beneficjenta.
2. O każdym przypadku naruszenia zabezpieczenia PEFS 2007 Administrator Bezpieczeństwa Informacji u Beneficjenta jest zobowiązany poinformować w formie pisemnej Administratora Bezpieczeństwa Informacji w IP/IP2.
3. 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 PEFS 2007 u Beneficjenta.

§ 17.

1. Kopie awaryjne danych osobowych przetwarzanych w PEFS 2007 są tworzone nie rzadziej niż raz na kwartał i zawierają pełny obraz danych osobowych w PEFS 2007 u Beneficjenta.
2. Kopie o których mowa w ust. 1 przechowuje się odpowiednio zabezpieczone przed dostępem osób nieuprawnionych w różnych miejscach, w tym w lokalizacjach innych niż zbiór danych osobowych eksploatowany na bieżąco.



§ 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, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego i kradnącego hasła odbywa się przy zastosowaniu zainstalowanego na każdej stacji roboczej aktualizowanego na bieżąco programu antywirusowego automatycznie monitorującego występowanie wirusów, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego, oprogramowania kradnącego hasła podczas operacji na plikach.

§ 20.

Nadzór nad instalowaniem oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

§ 21.

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

§ 22.

W ramach ochrony przed wrogim oprogramowaniem Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta stosuje logiczne lub fizyczne urządzenia firewall.

§ 23.

Dyski lub inne informatyczne nośniki zawierające dane osobowe przetwarzane w PEFS 2007 są przechowywane w sposób uniemożliwiający dostęp do nich osobom innym niż użytkownicy.

§ 24.

1. Żadne nośniki informacji zawierające dane osobowe nie są udostępniane poza obszar, w którym są przetwarzane dane osobowe.
2. Zapis w ust. 1 nie dotyczy sytuacji, o której mowa w § 29 pkt 1 ustawy o ochronie danych osobowych, tzn. udostępniania posiadanych w zbiorze danych osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, w szczególności przekazania przez Beneficjenta danych z PEFS 2007 właściwej Instytucji Pośredniczącej/Instytucji Pośredniczącej II Stopnia.



Rozdział 7

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

§ 25.

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 PEFS 2007 u Beneficjenta.

§ 26.

1. 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.
2. W przypadku niemożliwości usunięcia nośnika lub pozbawienia go zapisu tych danych osobowych naprawy dokonuje się pod nadzorem Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

§ 27.

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

§ 28.

Dostęp do danych osobowych przetwarzanych w PEFS 2007 jest dozwolony jedynie po właściwym zalogowaniu się i podaniu własnego hasła użytkownika.

Rozdział 9

Wymagania sprzętowo-organizacyjne

§ 29.

1. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.
2. Komputery powinny zostać ustawione w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną użytkowników.



§ 30.

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.

31.

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

Rozdział 10

Postanowienia końcowe

§ 32.

Do spraw nieuregulowanych w Instrukcji stosuje się przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych.



**załącznik nr 2
do zarządzenia nr 201/13
Wójta Gminy Suwałki
z dnia 22 lipca 2013 roku**

**Polityka Bezpieczeństwa
dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego
2007 dla PO KL w Gminie Suwałki**

**Rozdział 1
Postanowienia ogólne
§ 1.**

Polityka Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki, zwana dalej „Polityką”, określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w systemie Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Suwałki.

§ 2.

Użyte w Polityce określenia oznaczają:

- 1) Administrator Danych** - Instytucję Zarządzającą PO KL;
- 2) ustawa** - ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);
- 3) rozporządzenie** - rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
- 4) użytkownik** - osobę upoważnioną do przetwarzania danych osobowych w PEFS 2007;

- 5) **Administrator Bezpieczeństwa Informacji** - osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007;
- 6) **Administrator Bezpieczeństwa Informacji PEFS 2007 w IP/IP2** - osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 w IP/IP2;
- 7) **Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta** - osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta odpowiedzialną za sprawność, konserwację, wdrażanie technicznych zabezpieczeń PEFS 2007 oraz nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 u Beneficjenta;
- 8) **PEFS 2007** - Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL;
- 9) **naruszenie zabezpieczenia PEFS 2007** - jakiegokolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności PEFS 2007;
- 10) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 11) **przetwarzanie danych osobowych** - jakiegokolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych;
- 12) **usuwanie danych osobowych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

- 13) zbiór danych osobowych** - posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- 14) zabezpieczenie danych osobowych** - środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą;
- 15) Instrukcja** - Instrukcję Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki;
- 16) Pracownik** - osobę zatrudnioną u Beneficjenta na podstawie stosunku pracy lub stosunku cywilnoprawnego;
- 17) Ministerstwo** - Ministerstwo Rozwoju Regionalnego.

Rozdział 2

Zakres oraz zasady zabezpieczania danych osobowych

§ 3.

Niniejszą politykę stosuje się do zbioru danych osobowych PEFS 2007 znajdującego się w Gminie Suwałki.

§ 4.

1. Nadzór ogólny nad realizacją przepisów wynikających z ustawy oraz rozporządzenia pełni Administrator Danych.
2. Nadzór nad poprawnością realizacji przepisów o ochronie danych osobowych, w szczególności zasad opisanych w Polityce oraz Instrukcji, oraz nad wykonywaniem zadań związanych z ochroną danych osobowych w PEFS 2007 u Beneficjenta, sprawuje Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

§ 5.

Dane osobowe przetwarzane w PEFS 2007 podlegają ochronie zgodnie z przepisami ustawy.



§ 6.

Przetwarzanie danych osobowych w PEFS 2007 jest dopuszczalne wyłącznie w zakresie niezbędnym do udzielenia wsparcia, realizacji projektów, ewaluacji, monitoringu, sprawozdawczości i kontroli, w ramach Programu Operacyjnego Kapitał Ludzki.

§ 7.

Przetwarzanie danych osobowych w PEFS 2007 nie może naruszać praw i wolności osób, których dane osobowe dotyczą, a w szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących wskazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 8.

W przypadku zbierania jakichkolwiek danych osobowych na potrzeby PEFS 2007 bezpośrednio od osoby, której dane dotyczą, osoba zbierająca dane osobowe jest zobowiązana do przekazania tej osobie informacji o:

- 1) pełnej nazwie Ministerstwa oraz jego adresie;
- 2) celu zbierania danych osobowych;
- 3) prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;
- 4) dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożnością wzięcia udziału w projekcie realizowanym w ramach Programu Operacyjnego Kapitał Ludzki.

§ 9.

1. Jakiegokolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie określonym w ustawie oraz w pełnej zgodności z przepisami prawa.
2. Wnioski o udostępnienie danych osobowych przetwarzanych w PEFS 2007, po wstępnym rozpatrzeniu przez Administratora Bezpieczeństwa Informacji, są rozpatrywane przez Administratora Danych.

§ 10.

1. Przetwarzanie danych osobowych znajdujących się w PEFS 2007 może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 6, pod warunkiem zawarcia z tym podmiotem pisemnej umowy lub porozumienia, w pełni respektujących przepisy ustawy, rozporządzenia oraz umowy o dofinansowanie projektu.
2. Umowy lub porozumienia o powierzeniu przetwarzania danych osobowych w PEFS 2007 powinny zostać przed podpisaniem, w zakresie dotyczącym zasad przetwarzania danych osobowych, zaopiniowane przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.



§ 11.

Każdej osobie, której dane osobowe są przetwarzane w PEFS 2007 przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

- 1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;
- 2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
- 3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
- 4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
- 5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
- 6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

§ 12.

Na wniosek osoby, której dane osobowe dotyczą, Beneficjent jest zobowiązany, w terminie maksymalnie 30 dni od dnia wpłynięcia wniosku do Beneficjenta, wskazać w powszechnie zrozumiałej formie:

- 1) jakie dane osobowe dotyczące zapytującej osoby są przetwarzane przez Beneficjenta w PEFS 2007;
- 2) w jaki sposób zebrano te dane osobowe;
- 3) w jakim celu i zakresie te dane osobowe są przetwarzane;
- 4) od kiedy są przetwarzane te dane osobowe;
- 5) w jakim zakresie oraz komu te dane osobowe zostały udostępnione.

§ 13.

W razie wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe, przetwarzane przez Beneficjenta w PEFS 2007 są niekompletne, nieaktualne, nieprawdziwe, lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, w jakim zostały zebrane, Beneficjent jest zobowiązany do uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych osobowych lub ich usunięcia, zgodnie z żądaniem osoby, której dane osobowe dotyczą.

Rozdział 4

Obowiązki Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta

§ 14.

Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych w PEFS 2007 u Beneficjenta.



§ 15.

Do zadań Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta należy w szczególności:

- 1) współdziałanie z Administratorem Bezpieczeństwa Informacji PEFS 2007 w IP/IP2 w zakresie zapewniającym wypełnianie przez Beneficjenta obowiązków wynikających z ustawy i rozporządzenia;
- 2) prowadzenie i aktualizacja rejestru, o którym mowa w § 20, który stanowi załącznik nr 1 do Polityki;
- 3) prowadzenie i aktualizacja wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w PEFS 2007 u Beneficjenta, który stanowi załącznik nr 2 do Polityki;
- 4) analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych w ramach PEFS 2007 u Beneficjenta oraz pisemne informowanie o wynikach analizy osoby upoważnione do podejmowania decyzji w imieniu Beneficjenta;
- 5) opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych w PEFS 2007 podmiotowi zewnętrznemu wobec Beneficjenta;
- 6) inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych w PEFS 2007 u Beneficjenta.

§ 16.

W doborze i stosowaniu środków ochrony danych osobowych w PEFS 2007 Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta zwraca szczególną uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem lub nieuprawnioną modyfikacją.

§ 17.

1. Obowiązki Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta wykonywane są przez wyznaczonego przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta Pracownika.
2. Nadzór nad wykonywaniem obowiązków Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta pełni osoba upoważniona do podejmowania decyzji w imieniu Beneficjenta.

§ 18.

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania u Beneficjenta danych osobowych w PEFS 2007, Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta konsultuje się i współpracuje z Administratorem Bezpieczeństwa Informacji PEFS 2007 w IP/IP2.

Rozdział 5 **Przetwarzanie danych osobowych**

§ 19.

1. Do przetwarzania danych osobowych w PEFS 2007 mogą być dopuszczeni jedynie pracownicy posiadający odpowiednie upoważnienie wydane przez upoważnioną do tego osobę. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w załącznikach do umowy o dofinansowanie projektu.



2. Każdy pracownik, przed dopuszczeniem go do przetwarzania danych osobowych w PEFS 2007, musi być zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją.
3. Pracownik potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją przez złożenie podpisu na liście prowadzonej przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta, której wzór jest określony w załączniku nr 3 do Polityki.

§ 20.

1. Każdy pracownik mający dostęp do danych osobowych w PEFS 2007 jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Rejestr, o którym mowa w ust. 1, zawiera:
 - 1) imię i nazwisko pracownika;
 - 2) jego identyfikator w systemie informatycznym służącym przetwarzaniu danych w PEFS 2007;
 - 3) zakres przydzielonego uprawnienia;
 - 4) datę przyznania uprawnień;
 - 5) podpis Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta potwierdzający przyznanie uprawnień;
 - 6) datę odebrania uprawnień;
 - 7) podpis Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta potwierdzający odebranie uprawnień.

§ 21.

1. Dopuszczenie do przetwarzania danych osobowych znajdujących się w PEFS 2007 przez osoby niebędące pracownikami, jest możliwe tylko w wyjątkowych przypadkach, po uzyskaniu pozytywnej opinii Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych. W takim przypadku § 19 i 20 stosuje się odpowiednio.
2. Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 22.

Wszyscy pracownicy oraz osoby, o których mowa w § 21 ust. 1, pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych w PEFS 2007 danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

§ 23.

Użytkownicy są w szczególności zobowiązani do:

- 1) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w PEFS 2007, określonych w Polityce, Instrukcji i innych procedurach, dotyczących zarządzania PEFS 2007 oraz jego obsługi;
- 2) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach);
- 3) zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed

dostępem osób nieupoważnionych za pomocą środków określonych w Polityce, Instrukcji i innych procedurach dotyczących zarządzania PEFS 2007 oraz jego obsługi;

- 4) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
- 5) nieudzielania informacji o danych osobowych przetwarzanych w PEFS 2007 innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
- 6) bezzwłocznego zawiadamiania Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych w PEFS 2007, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

§ 24.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych są określone w załączniku nr 4 do Polityki.

Rozdział 6

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 25.

Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

- 1) stwierdzono naruszenie zabezpieczenia PEFS 2007;
- 2) stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych;
- 3) inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych w PEFS 2007.

§ 26.

1. Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych w PEFS 2007, jest zobowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:
 - 1) poinformować pisemnie o zaistniałym zdarzeniu Administratora Bezpieczeństwa Informacji PEFS 2007 w IP/IP2 i stosować się do jego zaleceń;
 - 2) zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu.
3. Administrator Bezpieczeństwa Informacji u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych w PEFS 2007 jest zobowiązany niezwłocznie:
 - 1) wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i podpisać;
 - 2) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę



- zniszczeń, metody dostępu osoby niepowołanej do danych osobowych w systemie informatycznym służącym przetwarzaniu danych osobowych w PEFS 2007;
- 3) podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony danych osobowych, w szczególności przez:
 - a) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej,
 - b) wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
 - c) zmianę hasła użytkownika, przez którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu;
 - 4) szczegółowo analizować stan systemu informatycznego służącego przetwarzaniu danych osobowych w PEFS 2007 w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;
 - 5) przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych w PEFS 2007.

§ 27.

1. Po przywróceniu normalnego stanu PEFS 2007 należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
2. Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych w PEFS 2007.
3. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym niebezpiecznym oprogramowaniem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
4. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań Beneficjenta, a w przypadku gdy użytkownik nie jest pracownikiem, konsekwencje wynikające z umowy, o której mowa w § 21 ust. 1.

§ 28.

1. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia PEFS 2007 i w terminie 21 dni od daty powzięcia wiedzy o naruszeniu zabezpieczenia PEFS 2007 przekazuje go Administratorowi Bezpieczeństwa Informacji w IP/IP2.
2. Jeżeli naruszenie zabezpieczenia PEFS 2007 nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych w PEFS 2007 Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta przygotowuje raport, o którym mowa w ust. 1.

Rozdział 7

Kontrola nad przestrzeganiem ochrony danych osobowych

§ 29.

1. Bieżąca kontrola nad przetwarzaniem danych osobowych w PEFS 2007 u Beneficjenta jest dokonywana przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.



2. W ramach kontroli, o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

§ 30.

1. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta przeprowadza w pierwszym kwartale roku kalendarzowego kontrolę w zakresie przestrzegania przez użytkowników Polityki, Instrukcji oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport.
2. Przygotowując raport, o którym mowa w ust. 1, Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta uwzględnia informacje zawarte w raportach, o których mowa w § 28.

§ 31.

Kontrola, o której mowa w § 30, polega w szczególności na sprawdzeniu:

- 1) którzy pracownicy mają dostęp do danych osobowych;
- 2) czy dane osobowe nie zostały udostępnione nieupoważnionym pracownikom lub osobom;
- 3) czy pracownicy i inne osoby mające dostęp do danych osobowych przetwarzanych w PEFS 2007 posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę.

Rozdział 8 Postanowienia końcowe

§ 32.

Polityka jest dokumentem wewnętrznym Beneficjenta i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§ 33.

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

§ 34.

Wykazy i rejestry znajdujące się w załącznikach nr 1-3 do Polityki, prowadzi Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

1. Wykaz znajdujący się w załączniku nr 4 do Polityki prowadzi w zakresie środków organizacyjnych i technicznych Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

§ 35.

Integralną część niniejszej Polityki stanowią następujące załączniki:

- 1) Załącznik nr 1 – Rejestr osób upoważnionych do przetwarzania danych osobowych w PEFS 2007 u Beneficjenta PO KL;
- 2) Załącznik nr 2 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe w PEFS 2007;
- 3) Załącznik nr 3 – Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;
- 4) Załącznik nr 4 -Określenie środków technicznych i organizacyjnych niezbędnych dla



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w PEFS 2007 u Beneficjenta;

- 5) Załącznik nr 5 – Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych w ramach PEFS 2007;
- 6) Załącznik nr 6 – Opis struktury zbioru danych PEFS 2007 wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- 7) Załącznik nr 7 – Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.



Załącznik nr 1

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
dla PO KL w Gminie Suwałki

Rejestr osób upoważnionych do przetwarzania danych osobowych w PEFS 2007 u Beneficjenta PO KL

Lp.	Imię i nazwisko	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data przyznania uprawnień	Podpis ABI PEFS 2007 u Beneficjenta	Data odebrania uprawnień	Podpis ABI PEFS 2007 u Beneficjenta
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							



UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla
PO KL w Gminie Suwałki

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe w PEFS 2007

[illegible]

Załącznik nr 3

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
dla PO KL w Gminie Suwałki

Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych

Oświadczam, iż zapoznałem/am się z:

- przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz przepisami wykonawczymi do niniejszej ustawy,
- Polityką Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki oraz z Instrukcją Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 dla PO KL w Gminie Suwałki.

Lp.	Imię i nazwisko	Data	Podpis potwierdzający zapoznanie się z ww. dokumentami
1			
2			
3			
4			
5			



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Lp.	Imię i nazwisko	Data	Podpis potwierdzający zapoznanie się z ww. dokumentami
6			
7			



Załącznik nr 4

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
dla PO KL w Gminie Suwałki

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w PEFS 2007 w Gminie Suwałki

I. Środki ochrony fizycznej danych:

- a) klucze do pomieszczeń wydawane wyłącznie osobom upoważnionym,**
- b) podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz,**
- c) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
- d) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych,
- e) zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej szafie,
- f) kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej szafie,
- g) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

II. Środki sprzętowe, informatyczne i telekomunikacyjne:

- a) Sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego chroniącego zasoby beneficjenta.
- b) Oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie.
- c) Dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- d) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- e) Zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe.

III Środki organizacyjne:

- a) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.



- b) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy.
- c) Monitory komputerów, na których są przetwarzane dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- d) Kopie zapasowe zbioru danych osobowych są przechowywane w innym pomieszczeniu niż to, w którym znajduje się komputer, na którym dane osobowe są przetwarzane na bieżąco.

Załącznik nr 5

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
dla PO KL w Gminie Suwałki

Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych w ramach PEFS 2007

Procedura przekazywania IP/IP2 Formularza PEFS 2007 przez Beneficjentów*

Formularz PEFS 2007 powinien zostać dostarczony na płycie CD lub innym nośniku danych do właściwej instytucji, do której składany jest wniosek beneficjenta o płatność, **osobiście lub przesłany pocztą tradycyjną za potwierdzeniem odbioru.**

Przekazywane dane powinny zostać uprzednio skompresowane do jednego z formatów: ZIP, TAR, GZ lub RAR oraz zabezpieczone hasłem z wykorzystaniem programu 7-Zip lub WinRAR. Użycie innego programu kompresującego jest dopuszczalne pod warunkiem, że instytucja do której składany jest wniosek o płatność wraz z Formularzem PEFS 2007 dysponuje adekwatnym narzędziem dekompresującym.

Hasło, przy użyciu którego zostaną zabezpieczone dane, powinno zostać przekazane do instytucji, do której dane będą kierowane w odrębnej niż zabezpieczony Formularz przesyłce. Niedopuszczalne jest przysyłanie Formularza PEFS 2007 z danymi pocztą elektroniczną.

Niestosowanie się do w/w procedury będzie uznawane przez IZ za rażące naruszenie przepisów o ochronie danych osobowych.

*Analogiczną procedurę należy stosować w przypadku wypełnienia Formularza PEFS 2007 przez podwykonawcę i przesyłania go do Beneficjenta.



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Załącznik nr 7

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
dla PO KL w Gminie Suwałki

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Zbiór danych osobowych:

- Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007

Programy zastosowane do przetwarzania danych osobowych:

- Formularz PEFS 2007

