Zarządzenie Nr 102 / 2012
Burmistrza Miasta i Gminy Kępno
z dnia 24 września 2012 r.

w sprawie przyjęcia polityki bezpieczeństwa dla zbioru danych Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych - Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Kępno w ramach realizacji projektu systemowego „Szkoła możliwości" POKL.09.01.02-30-313/10

Na podstawie art. 36 ust. 2 w związku z art. 31 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238, z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497 oraz z 2011 r. Nr 230, poz. 1371) oraz § 3-5 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 przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024) **zarządza się, co następuje :**

§ 1

1. Zatwierdzić i przyjąć do stosowania politykę bezpieczeństwa dla zbioru danych Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Kępno w ramach realizacji projektu systemowego „Szkoła możliwości" POKL.09.01.02-30-313/10, w brzmieniu załącznika Nr 1 do niniejszego zarządzenia.
2. Zatwierdzić i przyjąć do stosowania instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych - Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Kępno w ramach realizacji projektu systemowego „Szkoła możliwości" POKL.09.01.02-30-313/10, w brzmieniu załącznika Nr 2 do niniejszego zarządzenia.
3. Projekt „Szkoła możliwości" współfinansowany jest ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego z Programu Operacyjnego Kapitał Ludzki, priorytet IX Rozwój wykształcenia i kompetencji w regionie, Poddziałanie 9.1.2 Wyrównywanie szans edukacyjnych uczniów z grup o utrudnionym dostępnie do edukacji oraz zmniejszenie różnic w jakości usług edukacyjnych.

§ 2

Wykonanie zarządzenia powierza się Koordynatorowi Projektu oraz dyrektorom szkół podstawowych, dla których organem prowadzącym jest Burmistrz Miasta i Gminy Kępno, biorących udział w projekcie systemowym „Szkoła możliwości" POKL.09.01.02-30-313/10.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Aniela Kempa

Sp. M. Frala-Kędzior

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Załącznik nr 1
do zarządzenia Nr ...../2012
Burmistrza Miasta i Gminy Kępno
z dnia ..... września 2012 r. w sprawie
przyjęcia polityki bezpieczeństwa dla zbioru
danych Podsystem Monitorowania
Europejskiego Funduszu Społecznego 2007
oraz instrukcji zarządzania systemem
informatycznym służącym do przetwarzania
danych osobowych - Podsystem
Monitorowania Europejskiego Funduszu
Społecznego 2007 w Gminie Kępno w
ramach realizacji projektu systemowego
„Szkoła możliwości"
POKL.09.01.02-30-313/10

POLITYKA BEZPIECZEŃSTWA DLA ZBIORU DANYCH PODSYSTEM MONITOROWANIA EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO 2007 W GMINIE KĘPNO

Rozdział 1
Postanowienia ogólne
§ 1.

Polityka bezpieczeństwa dla zbioru danych Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Kępno, zwana dalej „**Polityką**", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorze danych Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007, zwanym dalej „**PEFS 2007**", w ramach realizacji projektu systemowego „Szkoła możliwości" POKL.09.01.02-30-313/10 w Gminie Kępno w woj. wielkopolskim.

§ 2.

Użyte w Polityce określenia oznaczają :

1) **Administrator Danych** – Ministerstwo Rozwoju Regionalnego pełniące funkcję Instytucji Zarządzającej dla Programu Operacyjnego Kapitał Ludzki;
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) **Beneficjent** – Gminę Kępno w woj. wielkopolskim;

5) **umowa** – umowa o dofinansowanie Projektu systemowego „Szkoła możliwości" w ramach Programu Operacyjnego Kapitał Ludzki współfinansowanego ze środków Europejskiego Funduszu Społecznego, zawarta w dniu 13 marca 2011 r. pomiędzy Samorządem Województwa Wielkopolskiego, zwanym dalej Instytucją Pośredniczącą, a Beneficjentem;
6) **Program** – Program Operacyjny Kapitał Ludzki zatwierdzony decyzją Komisji Europejskiej z dnia 28 września 2007 r. nr K (2007) 4547, zmienioną decyzją z dnia 21 sierpnia 2009 r. nr K (2009) 6607;
7) **Poddziałanie** – Poddziałanie 9.1.2. Wyrównywanie szans edukacyjnych uczniów z grup o utrudnionym dostępie do edukacji oraz zmniejszanie różnic w jakości usług edukacyjnych w ramach Programu;
8) **Projekt systemowy** – projekt systemowy pt. „Szkoła możliwości" realizowany w ramach Poddziałania określony we wniosku o dofinansowanie projektu systemowego nr POKL.09.01.02-30-313/10, stanowiącym załącznik nr 1 do umowy;
9) **użytkownik** - osobę upoważnioną do przetwarzania danych osobowych w PEFS 2007;
10) **Administrator Bezpieczeństwa Informacji** - osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007;
11) **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 Programu;
12) **Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta** - osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 u Beneficjenta, wyznaczoną przez Beneficjenta;
13) **Administrator Systemu u Beneficjenta** - osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych w PEFS 2007 u Beneficjenta, o ile zadania te zostały wyłączone z zakresu kompetencji Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta i powierzone przez Beneficjenta innemu pracownikowi;
14) **naruszenie zabezpieczenia PEFS 2007** - jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności PEFS 2007;
15) **dane osobowe** – dane osobowe w rozumieniu ustawy, dotyczące uczestników projektu systemowego, które muszą być przetwarzane przez Instytucję Pośredniczącą oraz Beneficjenta w celu wykonania Porozumienia w sprawie Realizacji Komponentu Regionalnego dla Programu Operacyjnego Kapitał Ludzki nr KL/WP/2007/1 zawartego w dniu 22 czerwca 2007 r., w zakresie określonym w załączniku nr 2 do umowy;
16) **przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym PEFS 2007;
17) **usuwanie danych osobowych** – usuwanie danych, o którym mowa w ustawie;
18) **zbiór danych osobowych** – zbiór danych, o którym mowa w ustawie;
19) **zabezpieczenie danych osobowych** – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
20) **Instrukcja** - instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych - Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007w Gminie Kępno;

21) **Pracownik** - osobę świadczącą pracę na rzecz Beneficjenta na podstawie stosunku pracy lub stosunku cywilnoprawnego;
22) **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 u Beneficjenta.

§ 4.

1. Nadzór ogólny nad realizacją przepisów 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 jest dopuszczalne wyłącznie w zakresie niezbędnym do udzielenia wsparcia, realizacji Projektu systemowego, ewaluacji, monitoringu, sprawozdawczości i kontroli, w ramach Programu, w zakresie określonym w załączniku nr 2 do umowy.

§ 7.

Przetwarzanie danych osobowych 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 skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 8.

1. Przetwarzanie danych osobowych jest dopuszczalne jeżeli osoba, której dane dotyczą, wyrazi zgodę na ich przetwarzanie. Osoba zbierająca dane osobowe jest zobowiązana do przekazania osobie, której dane dotyczą, 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 niewyrażenie zgody na ich przetwarzanie skutkuje niemożnością udzielenia wsparcia w ramach Projektu systemowego.
2. Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych stanowi załącznik nr 6 do umowy. Oświadczenia przechowuje Beneficjent w swojej siedzibie.

§ 9.

1. Jakiekolwiek 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, po wstępnym rozpatrzeniu przez Administratora Bezpieczeństwa Informacji, są rozpatrywane przez Administratora Danych.

§ 10.

1. Przetwarzanie danych osobowych 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.
2. Umowy lub porozumienia o powierzeniu przetwarzania danych osobowych 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 przysługuje prawo do kontroli przetwarzania jej danych osobowych, prawo do weryfikowania poprawności tych danych oraz sprzeciwienia się przetwarzaniu tych danych, szczegółowo określone w art. 32 – 35 ustawy.

Rozdział 4
Obowiązki Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta

§ 12.

Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta sprawuje nadzór nad przestrzeganiem zasad ochrony przetwarzania danych osobowych u Beneficjenta oraz realizuje inne zadania wynikające z Polityki.

§ 13.

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 § 18, którego wzór stanowi załącznik nr 1 do Polityki,
3) przygotowywanie projektów aktualizacji wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe u Beneficjenta, stanowiącego załącznik nr 2 do Polityki,
4) analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych u Beneficjenta oraz pisemne informowanie o wynikach analizy Beneficjenta,
5) opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu wobec Beneficjenta,
6) inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych u Beneficjenta.

§ 14.

W doborze i stosowaniu środków ochrony danych osobowych Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta zwraca szczególną uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 15.

1. Obowiązki Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta wykonywane są przez Pracownika wyznaczonego przez Beneficjenta.
2. Nadzór nad wykonywaniem obowiązków Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta i, o ile został powołany, Administratora Systemu u Beneficjenta pełni osoba upoważniona przez Beneficjenta.

§ 16.

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania u Beneficjenta danych osobowych, 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

§ 17.

1. Do przetwarzania danych osobowych mogą być dopuszczeni jedynie Pracownicy posiadający odpowiednie imienne upoważnienie do przetwarzania danych osobowych wydane przez Beneficjenta. Wzór imiennego upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w załącznikach 7-8 do umowy.
2. Każdy Pracownik, przed dopuszczeniem go do przetwarzania danych osobowych, 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.

§ 18.

1. Każdy Pracownik mający dostęp do danych osobowych 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.

§ 19.

1. Dopuszczenie do przetwarzania danych osobowych 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 § 17 i 18 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.

§ 20.

Wszyscy użytkownicy, pod groźbą sankcji wynikających z obowiązujących przepisów prawa, mają obowiązek zachowania tajemnicy o przetwarzanych danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

§ 21.

Użytkownicy są w szczególności zobowiązani do :

1) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych, 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 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, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe.

§ 22.

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

§ 23.

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.

§ 24.

1. Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, 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 PEFS 2007 u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych 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,
   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 celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
   5) przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych.
4. Czynności opisane w ust. 3 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 25.

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.
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 w stosunku do niego konsekwencje wynikające z odpowiednich przepisów prawa.

§ 26.

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 PEFS 2007 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 przygotowując raport, o którym mowa w ust. 1, współpracuje z Administratorem Systemu u Beneficjenta, o ile został powołany.

Rozdział 7
Kontrola nad przestrzeganiem ochrony danych osobowych

§ 27.

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.

§ 28.

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 § 26.

§ 29.

Kontrola, o której mowa w § 28, 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 posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę .

Rozdział 8
Postanowienia końcowe

§ 30.

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

§ 31.

Do spraw nieuregulowanych w Polityce stosuje się odpowiednie przepisy prawa, w szczególności przepisy o ochronie danych osobowych.

§ 32.

Polityka nie wyłącza stosowania przy przetwarzaniu danych osobowych innych instrukcji dotyczących zabezpieczenia PEFS 2007.

§ 33.

1. Wykazy i rejestry znajdujące się w załącznikach nr 1-3 do Polityki, prowadzi Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Wykaz znajdujący się w załączniku nr 4 do Polityki prowadzi w zakresie środków organizacyjnych Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta, zaś w zakresie środków technicznych Administrator Systemu u Beneficjenta, o ile został powołany.

§ 34.

Integralną część niniejszej Polityki stanowią następujące załączniki :

1) Załącznik nr 1 – Rejestr osób upoważnionych do przetwarzania danych osobowych w PEFS 2007 u Beneficjenta;
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 zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych 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 zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

KAPITAŁ LUDZKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Załącznik nr 1 do Polityki

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

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							

Załącznik nr 2 do Polityki

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

Lp.	Budynek – dane adresowe	Pomieszczenie

Załącznik nr 3 do Polityki

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

Oświadczam, iż zapoznałam/em 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 tej ustawy,
- Polityką bezpieczeństwa dla zbioru danych Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Kępno oraz z Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych - Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Kępno.

Lp.	Imię i nazwisko	Data	Podpis potwierdzający zapoznanie się z ww. dokumentami
1			
2			
3			
4			
5			
6			
7			

Załącznik nr 4 do Polityki

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych u Beneficjenta

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:

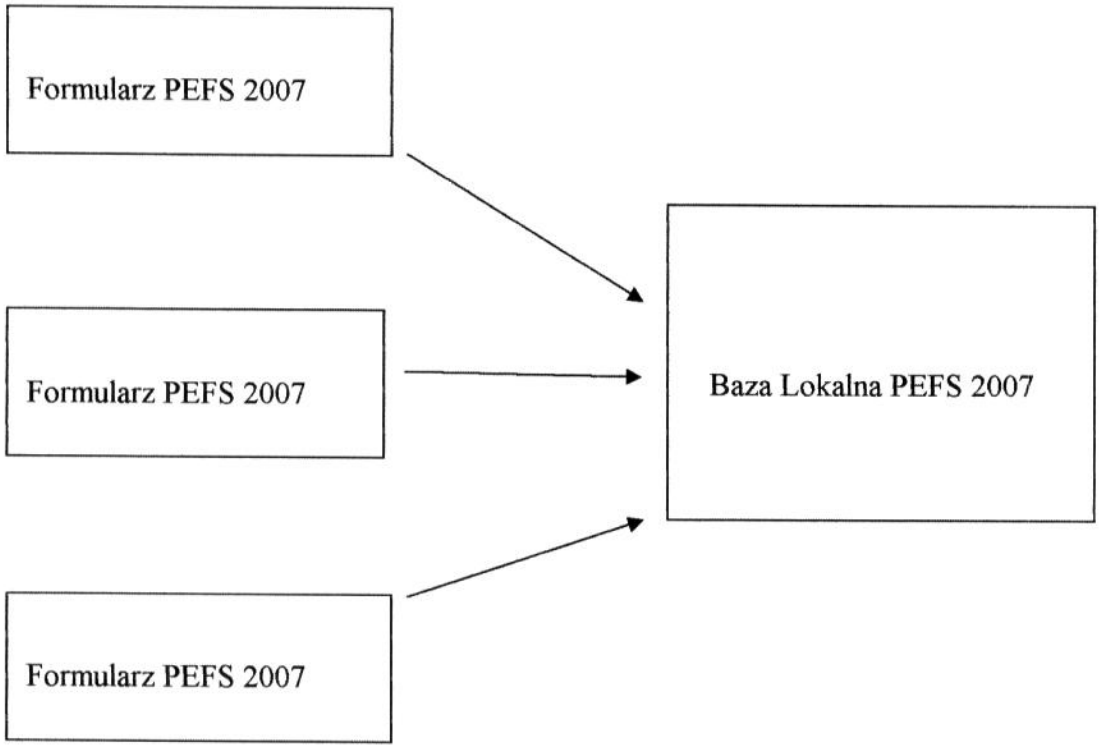
a) sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego chroniącego zasoby Beneficjenta,
b) oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki 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) użytkownicy zostali zaznajomieni z przepisami dotyczącymi ochrony danych osobowych,
b) użytkownicy zostali zobowiązani do zachowania danych osobowych 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

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 Win RAR. 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 przesyłanie 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.

Załącznik nr 6 do Polityki

Opis struktury zbioru danych PEFS 2007 wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Załącznik nr 7 do Polityki

Wykaz zbioru danych osobowych 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.

KAPITAŁ LUDZKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Załącznik nr 2
do zarządzenia Nr ...../2012
Burmistrza Miasta i Gminy Kępno
z dnia ..... września 2012 r. w
sprawie przyjęcia polityki
bezpieczeństwa dla zbioru
danych Podsystem Monitorowania
Europejskiego Funduszu
Społecznego 2007 oraz instrukcji
zarządzania systemem
informatycznym służącym do
przetwarzania danych osobowych –
Podsystem Monitorowania
Europejskiego Funduszu
Społecznego 2007 w Gminie Kępno
w ramach realizacji projektu
systemowego „Szkoła możliwości"
POKL.09.01.02-30-313/10

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH - PODSYSTEM MONITOROWANIA EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO 2007 W GMINIE KĘPNO

Rozdział 1
Postanowienia ogólne

§ 1.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych - Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Kępno, zwana dalej „**Instrukcją**", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych - Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007, zwanym dalej „**PEFS 2007**", w ramach realizacji projektu systemowego „Szkoła możliwości" POKL.09.01.02-30-313/10 w Gminie Kępno w woj. wielkopolskim.

§ 2.

Użyte w Instrukcji określenia oznaczają:

1) **Administrator Danych** – Ministerstwo Rozwoju Regionalnego pełniące funkcję Instytucji Zarządzającej dla Programu Operacyjnego Kapitał Ludzki;
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) **Beneficjent** – Gminę Kępno w woj. wielkopolskim;
4) **umowa** – umowa o dofinansowanie Projektu systemowego „Szkoła możliwości" w ramach Programu Operacyjnego Kapitał Ludzki współfinansowanego ze środków Europejskiego Funduszu Społecznego, zawarta w dniu 13 marca 2011 r. pomiędzy Samorządem Województwa Wielkopolskiego, zwanym dalej Instytucją Pośredniczącą, a Beneficjentem;

5) **Program** – Program Operacyjny Kapitał Ludzki zatwierdzony decyzją Komisji Europejskiej z dnia 28 września 2007 r. nr K (2007) 4547, zmienioną decyzją z dnia 21 sierpnia 2009 r. nr K (2009) 6607;
6) **Poddziałanie** – Poddziałanie 9.1.2. Wyrównywanie szans edukacyjnych uczniów z grup o utrudnionym dostępie do edukacji oraz zmniejszanie różnic w jakości usług edukacyjnych w ramach Programu;
7) **Projekt systemowy** – projekt systemowy pt. „Szkoła możliwości" realizowany w ramach Poddziałania określony we wniosku o dofinansowanie projektu systemowego nr POKL.09.01.02-30-313/10, stanowiącym załącznik nr 1 do umowy;
8) **dane osobowe** – dane osobowe w rozumieniu ustawy, dotyczące uczestników projektu systemowego, które muszą być przetwarzane przez Instytucję Pośredniczącą oraz Beneficjenta w celu wykonania Porozumienia w sprawie Realizacji Komponentu Regionalnego dla Programu Operacyjnego Kapitał Ludzki nr KL/WP/2007/1 zawartego w dniu 22 czerwca 2007 r., w zakresie określonym w załączniku nr 2 do umowy;
9) **przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym PEFS 2007;
10) **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 Programu Operacyjnego Kapitał Ludzki;
11) **Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta** - osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 u Beneficjenta;
12) **Administrator Systemu u Beneficjenta** - osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych - PEFS 2007 u Beneficjenta, o ile zadania te zostały wyłączone z zakresu kompetencji Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta i powierzone przez Beneficjenta innemu pracownikowi;
13) **naruszenie zabezpieczenia PEFS 2007** - jakiekolwiek zdarzenie lub działanie, które może stanowić przyczynę utraty zasobów, niezawodności, integralności lub poufności PEFS 2007;
14) **użytkownik** - osobę upoważnioną do przetwarzania danych osobowych w PEFS 2007;
15) **Polityka** - Politykę bezpieczeństwa dla zbioru danych Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Gminie Kępno.

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.

1. Osobą odpowiedzialną za przydział identyfikatorów i pierwszych haseł dla użytkowników u Beneficjenta jest Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 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. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.
3. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta prowadzi rejestr użytkowników, który stanowi załącznik nr 1 do Polityki.
4. Jakakolwiek zmiana informacji ujawnionych w rejestrze podlega natychmiastowemu odnotowaniu i uaktualnieniu.

§ 10.

W PEFS 2007 może zostać zarejestrowany jedynie użytkownik, któremu 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. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.
3. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta jest odpowiedzialny za zapoznanie każdego nowego użytkownika z Instrukcją oraz Polityką, a także z przepisami dotyczącymi ochrony danych osobowych, co użytkownik potwierdza swoim podpisem na liście, stanowiącej załącznik nr 3 do Polityki.

§ 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 zakończenia przez tego użytkownika współpracy z Beneficjentem na podstawie umowy cywilnoprawnej;
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 oraz Administratora Systemu u Beneficjenta, o ile został powołany.

2. O każdym przypadku naruszenia zabezpieczenia PEFS 2007 Administrator Bezpieczeństwa Informacji u Beneficjenta jest zobowiązany poinformować w formie pisemnej Administratora Bezpieczeństwa Informacji PEFS 2007 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.

1. 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.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 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.

1. Nadzór nad instalowaniem oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 21.

1. 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.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 22.

1. W ramach ochrony przed wrogim oprogramowaniem Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta stosuje logiczne lub fizyczne urządzenia firewall.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 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 udostępnia 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.

1. 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.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 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.
3. Nadzór opisany w ust. 2 sprawuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 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.

1. 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.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

Rozdział 10
Postanowienia końcowe

§ 32.

Do spraw nieuregulowanych w Instrukcji stosuje się odpowiednie przepisy prawa, w szczególności przepisy o ochronie danych osobowych.

§ 33.

Instrukcja nie wyłącza stosowania przy przetwarzaniu danych osobowych innych instrukcji dotyczących zabezpieczenia PEFS 2007.