Zarządzenie Nr 124/2011
Starosty Powiatu Wyszkowskiego
z dnia 04 października 2011 r.

w sprawie ustalenia „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie".

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.) oraz § 3 ust. 3 oraz § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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. z 2004 r. Nr 100, poz. l024) zarządzam, co następuje:

§ 1.

1. Ustala się „Politykę bezpieczeństwa i instrukcję zarządzania system informatycznym służącą do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie" zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik Nr 1 do niniejszego zarządzenia.
2. Ustala się „Politykę bezpieczeństwa dla zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w Starostwie Powiatowym w Wyszkowie Beneficjenta PO KL", która stanowi załącznik Nr 2 do niniejszego zarządzenia.

§ 2.

Zobowiązuje się pracowników Starostwa Powiatowego w Wyszkowie do stosowania zasad określonych w „Polityce bezpieczeństwa".

§ 3.

Traci moc Zarządzenie Nr 115/2007 Starosty Powiatu Wyszkowskiego z dnia 8 października 2007 r. w sprawie ustalenia „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie".

§ 4.

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia.

STAROSTA
Bogdan Mirosław Pągowski

Załącznik Nr 1
do zarządzenia Nr 124/2011
Starosty Powiatu Wyszkowskiego
z dnia 04 października 2011 r.

Polityka bezpieczeństwa

Opracował : Andrzej Hubert Morka
Administrator Bezpieczeństwa Informacji

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Starostwie Powiatowym w Wyszkowie. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18 poz. 162) oraz § 3 i 4 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).

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Starostwa Powiatowego w Wyszkowie.
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu.
4. Niniejszy dokument jest zgodny z następującymi aktami prawnymi:
   1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 103, poz. 929 z późn. zm.),
   2) Ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. Nr 11, poz. 95 z późn. zm.),
   3) Rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 171, poz. 1433),

Definicje

- **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
- **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);
- **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych;
- **System informatyczny** – system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, które dostarcza i rozprowadza informacje. Systemem informacyjnym może być system, w którym nie będzie żadnego komputera, a wyłącznie dokumenty papierowe, skoroszyty oraz ludzie tam pracujący, wyposażenie pokoi, czy też organizacja pracy. Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe;
- **Bezpieczeństwo systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
- **Starostwo** - Starostwo Powiatowe w Wyszkowie;
- **Administrator Danych Osobowych** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Starosta, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;
- **Administrator Bezpieczeństwa Informacji** – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
- **Administrator Systemów Informatycznych** – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych;
- **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;
- **Sieć Lokalna** – rozumie się przez to wewnętrzną sieć telekomunikacyjną;
- **Sieć rozległa** – rozumie się przez to zewnętrzną sieć publiczną;

- **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych, lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
  - osoby, której dane dotyczą,
  - osoby, upoważnionej do przetwarzania danych,
  - przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
  - podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
  - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

ROZDZIAŁ I

ZASADY POSTĘPOWANIA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Administrator Danych Osobowych, którym jest Starosta, zarządzeniem wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej Administrator Bezpieczeństwa Informacji oraz osobę upoważnioną do jego zastępowania.
2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych osobowych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   2) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   3) niezwłocznego informowania Administrator Danych Osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
3. Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje tylko w przypadku jego nieobecności.
4. Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego zastępstwa.
5. Pracownik upoważniony przez Administratora Danych Osobowych do przetwarzania danych osobowych, jest zobowiązany do:
   1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   2) stosowania określonych przez Administratora Danych Osobowych procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   3) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,
   4) podporządkowania się poleceniom Administratora Bezpieczeństwa Informacji oraz właściwego kierownika, w zakresie ochrony danych.
6. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych Osobowych. Wzór upoważnienia stanowi załącznik **Nr 1**.
7. Bezpośredni nadzór nad przetwarzaniem danych osobowych w wydziałach Starostwa sprawują kierownicy oraz naczelnicy tych wydziałów, a w przypadku pracowników na samodzielnych stanowiskach Starosta, Wicestarosta, Skarbnik – każdy w swoim pionie.
8. Naczelnicy wydziałów oraz stanowiska samodzielne w Starostwie są zobowiązani do:
   1) opracowania dla każdej osoby zatrudnionej przy przetwarzaniu danych osobowych zakresu czynności z uwzględnieniem stopnia dostępu do danych osobowych oraz przewidzenia odpowiedzialności, za naruszenie tajemnicy za danych, adekwatnej do zakresu obowiązków,
   2) sprawowanie nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,

3) zwracania się do administratora danych o rozstrzygnięcie w przypadku istotnych wątpliwości co do stosowania - przepisów prawnych zakresu danych osobowych,
4) niezwłocznego zawiadomienia Administratora Danych Osobowych o konieczności utworzenia nowego zbioru danych osobowych, wymagającego rejestracji.

9. Pracownik, któremu Administrator Danych Osobowych udzielił upoważnienia, o którym mowa w ust. 3 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi załącznik **Nr 2.**
10. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, bezpośredni przełożony jest zobowiązany bezzwłocznie skierować wniosek do Administratora Danych Osobowych o wydanie lub cofnięcie upoważnienia. W przypadku samodzielnych stanowisk pracy cofnięcia lub wydania upoważnienia dokonuje administrator danych. Wzór pisma o cofnięciu upoważnienia stanowi załącznik **Nr 3.**
11. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.
12. Naczelnik Wydziału Organizacyjnego i Spraw Społecznych przekazuje Administratorowi Bezpieczeństwa Informacji pisemna informację o rozwiązaniu umowy o pracę z pracownikiem posiadającym upoważnienie do przetwarzania danych osobowych.
13. W obiegu wewnętrznym między Wydziałami, referatami, a także pracownikami Starostwa wprowadza się następujące zasady udostępniania danych osobowych:
    1) informacje zawierające dane powszechnie dostępne może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „zwrotnej informacji telefonicznej",
    2) zgodę na udostępnienie danych osobowych w szerszym zakresie wyraża Starosta.
14. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych zgodnie z powszechnie obowiązującymi przepisami.
15. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.
16. Administrator Danych Osobowych może przenieść obowiązek utrzymywania lub przetwarzania zbioru/zbiorów danych osobowych, na podmiot trzeci jednak musi się to odbyć za pośrednictwem stosownej umowy oraz z zachowaniem reguł bezpieczeństwa danych opisanych w niniejszym dokumencie.
17. Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych.
18. Zbiory danych osobowych przetwarzane przez pracowników Starostwa nie będą udostępniane do celów komercyjnych.

Rozdział II

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:
    1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu, zakłócenia działania ciągłości systemu – nie dochodzi do naruszenia poufności danych,
    2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów,

administratora, awarie sprzętowe, błędy oprogramowania) – ich występowanie może doprowadzić do zniszczenia danych, zakłócenia ciągłość pracy systemu – może nastąpić naruszenie poufności danych,

3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. Naruszenie ochrony danych osobowych lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
   4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
   9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
   10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
   11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
   12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
   13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).
3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze

(wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział III

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem Danych Osobowych zawartych i przetwarzanych w systemach informatycznych Starostwa jest Starosta.
2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Starostwa, a w szczególności:
   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Celem zapewnienia ochrony przetwarzania danych w systemach informatycznych Starostwa stosuje się następujące środki techniczne:
   1) ochrona strefy administracyjnej systemem alarmowym klasy 2,
   2) przetwarzanie danych osobowych następuje w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   3) zabezpieczenie wejść do pomieszczeń, o których mowa w pkt. 1 w drzwi opatrzone w zamki,
   4) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   5) wyposażenie pomieszczeń w zamykane na klucz szafy dające gwarancję bezpieczeństwa dokumentacji.
4. Celem zapewnienia ochrony przetwarzania danych w systemach informatycznych Starostwa stosuje się następujące środki organizacyjne:
   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
   3) wyłączenie stref systemu alarmowego strefy administracyjnej przez upoważnione osoby,
   4) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez osobę upoważnioną, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.
5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.
6. Wykaz zbiorów przetwarzanych elektronicznie stanowi załącznik **Nr 4.**
7. Opis struktur zbiorów danych załącznik **Nr 5.**
8. Wykaz pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe zawiera załącznik **Nr 6.**

Rozdział IV

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych lub osoba przez niego wyznaczona, którą jest Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator Bezpieczeństwa Informacji sporządza półroczne plany kontroli zatwierdzone przez Starostę i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie i przedstawia Administratorowi Danych Osobowych.

ROZDZIAŁ V

ŚRODKI TECHNICZNE I ORGANIZACYJNE PRZEWIDZIANE DO OCHRONY DANYCH ZAWARTYCH W SYSTEMACH INFORMAYCZNYCH

1. Środki organizacyjne:
   1) dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez Administratora Danych Osobowych.
   2) każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych,
   3) należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych,
   4) pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz,
   5) dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy,
   6) dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu; w wypadku, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie pisemnego zezwolenia Administratora Danych Osobowych,
   7) dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu,
   8) w przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności,
   9) szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.
   10) klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy,
   11) szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane,
   12) dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.
2. Środki techniczne:
   1) dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu,

2) stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione,
3) każdy plik, w którym są zawarte dane osobowe powinien być zabezpieczony hasłem jeśli nie jest to przetwarzanie danych w systemie informatycznym,
4) w przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu,
5) po zakończeniu pracy komputery (notebook) powinny być zabezpieczone w zamykanych na klucz szafach,
6) komputerów nie należy wynosić poza budynek,
7) w wypadku potrzeby wyniesienia (notebook-a) wcześniej należy dane osobowe przenieść na komputer stacjonarny w miejscu pracy,
8) nie należy udostępniać osobom nieupoważnionym komputerów,
9) w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności i za zgodą Administratora Bezpieczeństwa Informacji,
10) nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe,
11) w wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy płytę zniszczyć fizycznie,
12) w przypadku wykorzystania do przenoszenia dysków, dane należy kasować z dysków,
13) niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną,
14) sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz,
15) do zabezpieczenia sieci należy stosować:
    a) firewall – zaporę sprzętową lub programową uniemożliwiającą dostęp osób nieuprawnionych z zewnętrznej sieci,
    b) adresowanie stacji roboczych tylko adresami prywatnymi,
    c) systemy wykrywania włamań,
    d) logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach,
    e) systemy antywirusowe,
    f) zabezpieczenia skrzynek poczty elektronicznej hasłami „trudnymi" (8 znaków w tym litery, cyfry, znaki dodatkowe),
    g) zabezpieczenie przed dostępem na zewnątrz ze stacji roboczych do innych usług niż strony internetowe,
    h) dostęp do poczty elektronicznej tylko na serwerach autoryzowanych przez Starostwo,
    i) zabezpieczenia stacji roboczych poprzez hasła na BIOS, w systemach MS Windows 2000, i XP poprzez użytkowników i hasła,
    j) zabezpieczenie wszelkich systemów teleinformatycznych hasłami „trudnymi" (8 znaków w tym litery, cyfry, znaki dodatkowe) zmienianymi raz na miesiąc,
    k) ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemach teleinformatycznych.

ROZDZIAŁ VI

INSTRUKCJA OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH, ZE SZCZEGÓLNYM UWZGLĘDNIENIEM BEZPIECZEŃSTWA INFORMACJI

1. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności:
   1) hasło nie powinno zawierać mniej niż 8 znaków,
   2) hasło nie może być takie samo jak identyfikator,
   3) hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika, administratora bezpieczeństwa informacji lub automatycznie przez system,
   4) użytkownikowi nie wolno zapisywać hasła na papierze,
   5) użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
   6) komputery nie pracujące w sieci muszą mieć hasło założone na BIOS,
   7) w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu, lub po 5 minutach musi uruchomić się wygaszacz ekranu zabezpieczony hasłem,
   8) za gospodarkę hasłami odpowiedzialny jest Administrator Bezpieczeństwa Informacji,
   9) hasło przy wpisywaniu nie może być wyświetlane na ekranie.
2. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności:
   1) Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych, zawierającą ich identyfikatory, wzór ewidencji stanowi załącznik **Nr 7,**
   2) rejestracji użytkowników w systemie dokonuje Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,
   3) zarejestrować można wyłącznie osoby, które administrator danych wpisał do ewidencji osób upoważnionych do przetwarzania danych,
   4) wyłączenie z ewidencji osób upoważnionych do przetwarzania danych, obliguje administratora bezpieczeństwa informacji do odebrania dostępu do danych osobowych,
   5) zalecane jest aby identyfikator składał się z pierwszej litery imienia i nazwiska.
3. Procedury rozpoczęcia i zakończenia pracy:
   1) Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Danych Osobowych, ustala czas pracy użytkownikom systemu, na pracę poza godzinami funkcjonowania urzędu musi wyrazić zgodę na piśmie Administrator Danych Osobowych, w formie upoważnienia jednorazowego lub stałego,
   2) Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, nadzoruje rozpoczęcie i zakończenie pracy systemu informatycznego,
   3) w pomieszczeniach gdzie przyjmowani są klienci , monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane,
   4) dopuszcza się pozostawianie włączonego serwera w nocy, jeżeli pomieszczenie w którym pracuje wyposażone jest w sprawny system powiadamiania przeciw pożarowego, zasilacza awaryjnego oraz alarm antywłamaniowy.
   5) kontrola wprowadzanych danych prowadzona jest na bieżąco na każdym stanowisku merytorycznym, nadzór prowadzi bezpośredni przełożony,

6) o przekazywaniu danych osobowych innym podmiotom decyduje Administrator Danych Osobowych,.
7) osoby, których dane są przetwarzane powinny mieć możliwość zapoznania się, na tablicy ogłoszeń, z przysługującymi im prawami wynikającymi z ustawy o ochronie danych osobowych.

4. Metoda i częstotliwość tworzenia kopii awaryjnych:
   1) za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,
   2) kopii należy dokonywać poprzez przegrywanie całej bazy danych,
   3) w każdej chwili powinno być dostępnych jednocześnie pięć kopii: z ostatniego dnia, tygodnia, miesiąca, kwartału i roku; kopie dzienne i tygodniowe należy zapisywać na dysku twardym, dyskach CD lub DVD a pozostałe na taśmach magnetycznych,
   4) kopie awaryjne może tworzyć jedynie Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,
   5) w czasie tworzenia kopii awaryjnej przez administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany,
   6) dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy,
   7) Administrator Bezpieczeństwa Informacji wykonuje kopię awaryjną lub archiwizacje systemu wykorzystując jak najlepiej swoje umiejętności,
   8) wprowadza się praktyczne zalecenia odnośnie do wykonania kopii bezpieczeństwa:
      a) przeprowadzić składowanie informacji regularnie,
      b) używać różnych typów nośników danych,
      c) kopie umieszczać w różnych, oddalonych od siebie miejscach,
      d) najlepiej do składowania wybrać tak nośnik, aby mógł w całości pomieścić kopie danych,
      e) przed składowaniem danych sprawdzić je programem antywirusowym,
      f) dokładnie opisywać składowane dane,
      g) trzymać nośniki z kopiami z daleka od źródeł pola magnetycznego i miejsc nasłonecznionych,
      h) sprawdzić, czy składowanie przebiegło prawidłowo,
      i) upewnić się, że nośnik jest niezależny od urządzenia, tzn. że dane mogą być przywrócone nie tylko na komputerze, z którego były poprawne,
      j) regularnie konserwować urządzenia do składowania.

5. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz metody ich usuwania:
   1) za ochronę antywirusową odpowiedzialny jest Administrator Bezpieczeństwa Informacji,
   2) do ochrony antywirusowej należy stosować jednostanowiskowy program antywirusowy, zainstalowany na komputerze, gdzie odbierana jest poczta elektroniczna i sprawdzane są wszystkie dyskietki i płyty CD, przed ich uruchomieniem w sieci oraz na komputerach wolno stojących,
   3) sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w miesiącu,
   4) zalecane jest wykorzystanie programów pracujących w tle,
   5) przy kontroli szczególną uwagę należy zwrócić na makra,
   6) każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym,
   7) korzystanie z zewnętrznych nośników informacji (dyskietek, dysków wymiennych, płyt CD, Internetu, poczty elektronicznej) może mieć miejsce wyłącznie po uzyskaniu

zgody Administratora Bezpieczeństwa Informacji,

8) w przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w Starostwie.

6. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków:
   1) nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych,
   2) za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest kierownik komórki organizacyjnej, za skasowanie danych, lub zniszczenie nośników elektronicznych, odpowiedzialny jest administrator bezpieczeństwa informacji,
   3) zbędne dokumenty konwencjonalne (papierowe) powinny być zniszczone w niszczarce dokumentów lub podarte na drobne fragmenty,
   4) kopie bezpieczeństwa powinny być przechowywane w zamkniętej metalowej szafie,
   5) kopie nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco,
   6) kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu – co najmniej jednorazowo po przegraniu,
   7) wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane,
   8) osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych, w szczególności komputera nie należy pozostawiać w samochodzie,
   9) kopie przechowuje się co najmniej:
      a) dzienne przez siedem dni,
      b) tygodniowe przez kolejny tydzień,
      c) miesięczne przez kolejny miesiąc,
      d) kwartalne przez kolejny kwartał,
      e) roczne przez cały kolejny rok od daty sporządzenia.

7. Przeglądu, konserwacji systemu i zbioru danych osobowych:
   1) przeglądu i konserwacji dokonuje Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona, przynajmniej dwa razy w roku,
   2) zasilacz awaryjny powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – min. czas podtrzymania pracy wynosi 5 min,
   3) w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez administratora danych, w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować,
   4) o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji,
   5) do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń (czajników elektrycznych, odkurzaczy,

radioodbiorników),
6) zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.

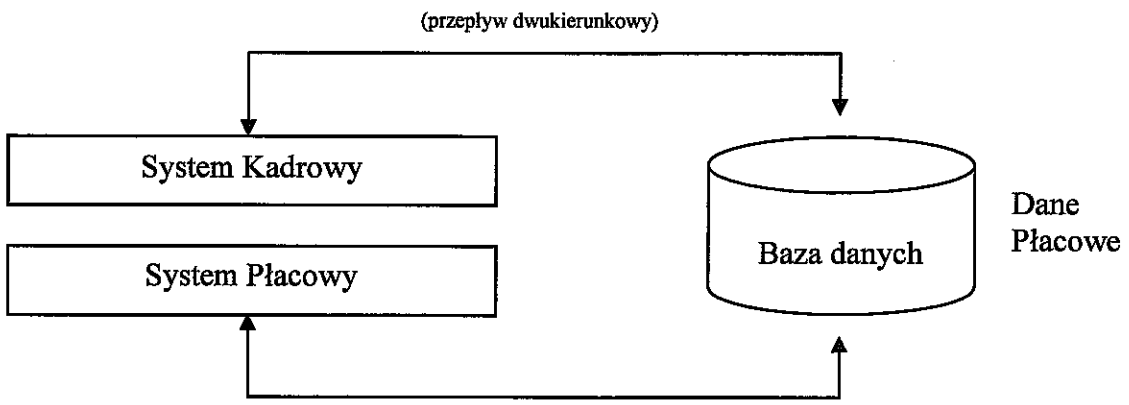
8. Sposób postępowania w zakresie komunikacji w sieci komputerowej:
   1) przy przydzielaniu uprawnień obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione",
   2) Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Danych Osobowych określi zasoby dostępne dla każdego użytkownika,
   3) użytkownicy powinni być przydzielani do odpowiedniej grupy roboczej, automatycznie w procesie logowania,
   4) dostęp do serwerowi ma tylko Administrator Bezpieczeństwa Informacji i pracownicy upoważnieni przez Administratora Danych Osobowych,
   5) dostęp do konsoli serwera winien być zabezpieczony hasłem,
   6) Administrator Bezpieczeństwa Informacji winien monitorować pracę w sieci za pomocą dostępnego oprogramowania narzędziowego i plików *.log,
   7) w pomieszczeniu, gdzie ustawiony jest serwer powinien pracować tylko Administrator Bezpieczeństwa Informacji i osoby upoważnione przez Administratora Danych Osobowych,
   8) nie wolno instalować w sieci własnego oprogramowania bez zgody Administratora Bezpieczeństwa Informacji,
   9) nieupoważnieni użytkownicy nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i wolumenów z poziomu systemu operacyjnego,
   10) dostęp do archiwalnych plików pocztowych należy zabezpieczyć hasłem,
   11) wszystkie listy otrzymane pocztą elektroniczną należy przekazywać do kancelarii,
   12) w celu zwiększenia bezpieczeństwa transmisji danych osobowych należy stosować kryptografie,
   13) w czasie korzystania z Internetu za pośrednictwem linii komutowanej, końcówka powinna być fizycznie odłączona od sieci lokalnej,
   14) uczestnictwo w internetowych grupach dyskusyjnych dozwolone jest jedynie za zgodą Administratora Danych Osobowych,
   15) komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników.

9. Sposób przepływu danych pomiędzy systemami:
   1) stacje robocze w Starostwie połączone są w sieć logiczną za pośrednictwem sieci Ethernet,
   2) w budynku Starostwa występują dwie podsieci na których są bazy zawierające dane osobowe,
   3) w systemie informatycznym Starostwa występują cztery serwery pełniące rolę bazodanowych w przypadku konieczności przetwarzania większych zbiorów lub udostępnienia na więcej niż jednej stacji roboczej; serwery znajdują się w pokoju nr 19; scentralizowanie położenia baz danych pozwala na lepszą kontrolę nad tworzeniem kopii zapasowych; w przypadkach gdy wymagania środowiska lub koszty uniemożliwiają umiejscowienie bazy na serwerze – system bazy danych uruchamiany jest na stacji roboczej, na której przetwarzane są dane,
   4) w Starostwie nie istnieją żadne relacje pomiędzy różnymi systemami informatycznymi,
   5) w przypadku zmiany stanu opisanego w punkcie 4 należy przedstawić w załączniku sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie

istnieją pomiędzy danymi zgromadzonymi w zbiorach do przetwarzania, których systemy te są wykorzystywane,

6) przepływ danych przedstawia schemat (rysunek nr 1), wskazuje on z jakimi zbiorami dany system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest jednokierunkowy (np. informacje pobierane są tylko do odczytu), czy dwukierunkowy (np. do odczytu i do zapisu),
7) w sposobie przepływu danych pomiędzy poszczególnymi systemami zamieszcza się informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (np. przy wykorzystaniu zewnętrznych nośników danych), lub półautomatycznie – za pomocą teletransmisji (np. przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu.

Rysunek nr 1



Rozdział VII

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

   każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.
2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, o naruszeniu ochrony danych osobowych należy powiadomić bezpośredniego przełożonego.
3. O naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:

8) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,.
9) brak możliwości zalogowania się do tej aplikacji,
10) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji.
11) wygląd aplikacji inny niż normalnie,
12) inny zakres danych niż normalnie dostępny dla użytkownika – dużo więcej lub dużo mniej danych,
13) znaczne spowolnienie działania systemu informatycznego,
14) pojawienie się nie standardowych komunikatów generowanych przez system informatyczny,
15) ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
16) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii awaryjnych,
17) włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej - nośniki danych osobowych,
18) zagubienie lub kradzież nośnika danych osobowych,
19) zagubienie lub kradzież nośnika, karty mikroprocesorowej, dyskietki, itp,
20) kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe.
21) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
22) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej,
23) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

4. Ujawnienie danych następuje gdy:
   1) stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą,
   2) dane zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.
5. Przypadki określone w ust. 4 wymagają przeprowadzenia postępowania wyjaśniającego które określi czy dane osobowe należy uznać za ujawnione.
6. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub upoważnionej przez Administratora Danych Osobowych osoby, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji

systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

7. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub osoba go zastępująca:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Starostwa,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych Osobowych lub Sekretarza Powiatu,
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Starostwa,
5) zapisać wszelkie informacje związane z danym zdarzeniem,
6) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
7) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
8) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,
9) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
10) dokonać zmiany hasła użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

8. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik **Nr 8**, który powinien zawierać w szczególności:
1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu i miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
5) wstępną ocenę przyczyn wystąpienia naruszenia,
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

9. Raport, o którym mowa w ust. 8, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych Osobowych, a w przypadku jego nieobecności osobie uprawnionej.

10. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

11. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Sekretarza Powiatu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

12. Analiza, o której mowa w ust. 10, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć

proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział VIII

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
   1) Administrator Danych Osobowych bądź upoważniona przez niego osoba,
   2) Administrator Bezpieczeństwa Informacji.
2. W ramach kontroli należy zwracać szczególna uwagę na:
   1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   2) kontrola ewidencji nośników magnetycznych,
   3) kontrola właściwej częstotliwości zmiany haseł .

Rozdział IX

SZKOLENIA

1. Wszyscy pracownicy Starostwa mają obowiązek brać udział w szkoleniach.
2. Szkolenie powinno dotyczyć:
   1) obowiązujących instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
   2) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

Rozdział X

NISZCZENIE ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji.
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.

Rozdział XI

ARCHIWIZACJA DANYCH

1. Dane systemów kopiowane są w systemie tygodniowym.
2. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie.

3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji.
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w kasie pancernej w pokoju wskazanym przez Administratora Danych Osobowych oraz skrytce bankowej.
5. Kopie awaryjne przechowywane są w kasie pancernej w pokoju wskazanym przez Administratora Danych Osobowych.
6. Dyskietki, na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane w taki sposób, by nie można było odtworzyć ich zawartości.
7. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny tak, by nie można było użyć ich ponownie.
8. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
9. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności.

Rozdział XII

ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Zbiory danych udostępnia się na pisemny, umotywowany wniosek (wzór wniosku stanowi załącznik **nr 9**), chyba że odrębne przepisy prawa stanowią inaczej.
3. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
4. Administrator Danych Osobowych kieruje wniosek do rozpatrzenia do wydziału merytorycznego, który jednocześnie prowadzi ewidencję wniosków.
5. Decyzję w sprawie udostępnienia danych podejmuje wyłącznie Administrator Danych Osobowych.
6. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli:
   1) spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób.
   2) dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.
7. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.
8. Podmiot, o którym mowa w ust. 7 jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie, w jakim reguluje to zawarta umowa.

Rozdział XIII

UDZIELANIE INFORMACJI O PRZETWARZANIU DANYCH OSOBOWYCH

1. Osobom, których dane przetwarza się w zbiorze danych Starostwa, przysługuje zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.
2. Każda osoba której dane przetwarzane są w zbiorze danych Starostwa przysługuje prawo 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.
3. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, musi otrzymać odpowiedź na piśmie w terminie nie przekraczającym 30 dni od daty wpłynięcia wniosku.
4. W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy o której mowa powyżej, albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział XIV

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik **nr 10** do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926), 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

6. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie" wchodzi w życie z dniem podpisania przez Starostę.

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 1

Wyszków, dnia .....

U P O W A Ż N I E N I E Nr.....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926)

u p o w a ż n i a m

.....
/imię i nazwisko/

zatrudnionego na stanowisku.....

do przetwarzania danych osobowych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

w.....
/nazwa jednostki organizacyjnej/

Upoważnienie wydaje się na czas nieokreślony.

.....
Administrator Danych Osobowych

STAROSTA
Tomasz Mirosław Pągowski

Załącznik nr 2

Wyszków, dnia .....

.....
/imię i nazwisko pracownika/

.....

.....
/adres zamieszkania/

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów :
   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
   b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926),
   c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych .

.....
(podpis pracownika)

.....
(podpis złożono w obecności)

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 3

Wyszków, dnia .....

Wycofanie upoważnienia

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
w związku:
.....
.....
.....

cofam upoważnienie

Pana/Pani .....
zatrudnionego/zatrudnionej w.....
.....
na stanowisku .....
.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

.....
Administrator Danych Osobowych

STAROSTA
Bogdan Mirosław Pagowski

Załącznik nr 4

Wykaz zbiorów przetwarzanych elektronicznie.

Lp.	Nazwa zbioru	Program zastosowany do przetwarzania	Nazwa urządzenia, w którym znajdują się dane osobowe
1	Komputerowy system rejestracji pojazdów, Ewidencja kierowców	Pojazd , Kierowca	Serwer
2	Powiatowy zasób Geodezyjny i Kartograficzny	Ośrodek	Serwer
3	Ewidencja gruntów i budynków m. Wyszków, Gm. Wyszków, Zabrodzie, Somianka, Długosiodło, Brańszczyk	EGB	Serwer

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 5

Struktury zbiorów danych

1. Zbiór danych „Powiatowy zasób Geodezyjny i Kartograficzny" zawiera następujące pola:

• imiona i nazwiska
• imiona rodziców
• adres zamieszkania lub pobytu

2. Zbiór danych „Oświadczenie o stanie mienia majątkowego" zawiera następujące pola:

• imiona i nazwiska
• data urodzenia
• adres zamieszkania lub pobytu
• miejsce pracy
• seria i numer dowodu osobistego

3. Zbiór danych „Plany urządzania lasów nie stanowiących własność Skarbu Państwa" zawiera następujące pola:

• imiona i nazwiska
• imiona rodziców
• adres zamieszkania lub pobytu

4. Zbiór danych „Ewidencja kart wędkarskich" zawiera następujące pola:

• imiona i nazwiska,
• data urodzenia
• adres zamieszkania lub pobytu
• numer i seria dowodu osobistego

5. Zbiór danych „Komputerowy system rejestracji pojazdów" zawiera następujące pola:

• imiona i nazwiska
• adres zamieszkania lub pobytu
• numer PESEL
• seria i numer dowodu osobistego

6. Zbiór danych „Ewidencja rozpoczynanych i oddawanych do użytkowania obiektów budowlanych" zawiera następujące pola:

• imiona i nazwiska,
• imiona rodziców
• adres zamieszkania lub pobytu

- seria i numer dowodu osobistego

7. Zbiór danych „Ewidencja pozwoleń wodno-prawnych" zawiera następujące pola:

- imiona i nazwiska,
- adres zamieszkania lub pobytu,

8. Zbiór danych „Ewidencja pozwoleń na budowę" zawiera następujące pola:

- imiona i nazwiska,
- imiona rodziców
- adres zamieszkania lub pobytu
- seria i numer dowodu osobistego

9. Zbiór danych „Ewidencja gruntów i budynków m. Wyszków, Gm. Wyszków, Zabrodzie, Somianka, Długosiodło, Brańszczyk" zawiera następujące pola:

- imiona i nazwiska,
- imiona rodziców
- adres zamieszkania lub pobytu
- numer PESEL

9. Zbiór danych „Ewidencja kierowców" zawiera następujące pola:

- imiona i nazwiska,
- data urodzenia
- adres zamieszkania lub pobytu
- numer PESEL
- seria i numer dowodu osobistego

10. Zbiór danych „Zmiana imion i nazwisk" zawiera następujące pola:

- imiona i nazwiska,
- imiona rodziców
- data urodzenia
- adres zamieszkania lub pobytu
- miejsce pracy
- zawód
- wykształcenie
- seria i numer dowodu osobistego

11. Zbiór danych „Rejestr wydanych licencji, zaświadczeń i zezwoleń na wykonywanie transportu drogowego w Starostwie Powiatowym w Wyszkowie" zawiera następujące pola:

- imiona i nazwiska,
- Numer Identyfikacji Podatkowej
- numer telefonu

12. Zbiór danych „Rejestr wydanych legitymacji osoby niepełnosprawnej, która nie ukończyła 16 roku życia" zawiera następujące pola:

• imiona i nazwiska,
• imiona rodziców
• data urodzenia
• miejsce urodzenia
• adres zamieszkania lub pobytu
• numer PESEL
• miejsce pracy
• zawód
• wykształcenie
• seria i numer dowodu osobistego
• numer telefonu

13. Zbiór danych „Rejestr wydanych legitymacji osoby niepełnosprawnej" zawiera następujące pola:

• imiona i nazwiska,
• imiona rodziców
• data urodzenia
• miejsce urodzenia
• adres zamieszkania lub pobytu
• numer PESEL
• miejsce pracy
• zawód
• wykształcenie
• seria i numer dowodu osobistego
• numer telefonu

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 6

Wykaz pomieszczeń lub części pomieszczeń, w których przetwarzane są dane.

Lp.	Nr pokoju	Wydział/ Referat/Sam. Stanowisko	Określenie części pomieszczenia, w którym przetwarza się lub archiwizuje dane
Budynek: Starostwo Powiatowe w Wyszkowie, ul. Aleja Róż 2 07-200 Wyszków			
1	15-18, 27	Wydział Komunikacji	Nie dotyczy
2	20-25	Wydział Geodezji i Gospodarki Nieruchomościami	Nie dotyczy
3	4,13	Wydział Planowania Rozwoju i Wdrażania Programów Pomocowych	Nie dotyczy
4	9-10	Wydział Architektoniczno - Budowlany	Nie dotyczy
5	8, 39	Wydział Organizacyjny i Spraw Społecznych	Nie dotyczy
Budynek: Starostwo Powiatowe w Wyszkowie, uł. Aleja Róż 1 07-200 Wyszków			
6	4	Wydział Ochrony Środowiska i Rolnictwa	Nie dotyczy
7	5	Powiatowy Zespół do Spraw Orzekania o Niepełnosprawności	Nie dotyczy

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 7

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

L.p.	Imię i Nazwisko	Nr upoważnienia	Identyfikator	Data, podpis

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 8

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego
w Starostwie Powiatowym w Wyszkowie

1. Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

.....
nr pokoju, nazwa pomieszczenia

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania:

.....
.....

6. Przyczyny wystąpienia zdarzenia:

.....
.....

7. Postępowanie wyjaśniające:

.....
.....

STAROSTA
Bogdan Mirosław Pągowski

.....
data, podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 9

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

Wniosek do .....

.....

(dokładne oznaczenie administratora danych)

1. Wnioskodawca .....

.....

.....

(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, NIP oraz nr REGON)

2. Wskazanie przeznaczenia dla udostępnionych danych:

.....

.....

.....

3. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:

.....

.....

.....

4. Zakres żądanych informacji ze zbioru:

.....

.....

.....

5. Informacje umożliwiające wyszukanie w zbiorze żądanych danych: .

.....

.....

.....

(miejsce na znaczki opłaty skarbowej) .....

(data i podpis, pieczęć wnioskodawcy)

STAROSTA
Bogdan Mirosław Pągowski

(data i podpis, pieczęć wnioskodawcy)

Załącznik nr 10

Wykaz osób, które zostały zapoznane i zobowiązują się do stosowania „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie" .

Imię i Nazwisko	Komórka organizacyjna	Data i podpis

STAROSTA
Bogdan Mirosław Pągowski

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Załącznik Nr 2
do Zarządzenia Nr 124/2011
Starosty Powiatu Wyszkowskiego
z dnia 04.X.2011 r.

POLITYKA BEZPIECZEŃSTWA DLA ZBIORU PODSYSTEM MONITOROWANIA EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO 2007 W STAROSTWIE POWIATOWYM W WYSZKOWIE BENEFICJENTA PO KL

Uzgodniono
dnia 26 września 2011 r.

Rozdział 1
Postanowienia ogólne

§ 1.

Polityka Bezpieczeństwa dla zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL, zwana dalej „Polityką", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorze Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007, zwanym dalej „PEFS 2007", **w Starostwie Powiatowym w Wyszkowie ,** zwanym dalej „Beneficjentem".

§ 2.

Użyte w Polityce określenia oznaczają:

1) **Administrator Danych** - Starosta Powiatu ;

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) **Beneficjent** - instytucja, która otrzymuje wsparcie objęta w ramach EFS tj. Starostwo Powiatowe w Wyszkowie

8) **Administrator Bezpieczeństwa Informacji PEFS 2007 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;

9) **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 osobę upoważnioną do podejmowania decyzji u Beneficjenta innemu pracownikowi;

10) **naruszenie zabezpieczenia PEFS 2007** - jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności PEFS 2007;

11) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

12) **przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych;

13) **usuwanie danych osobowych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

14) **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;

15) **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;

16) **Instrukcja** - Instrukcję Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta;

17) **Pracownik** - osobę zatrudnioną u Beneficjenta na podstawie stosunku pracy lub innego stosunku prawnego;

18) **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 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 skazań, 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. 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 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 i, o ile został powołany, Administratora Systemu 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.
4. Czynności opisane w ust. 3 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 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 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

§ 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 kalendarzowym 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.

Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia PEFS 2007.

§ 35.

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.

§ 36.

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 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.

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 1

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL

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

STAROSTA

Bogdan Mirosław Pogowski

Załącznik nr 2

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL

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

Lp.	Budynek – dane adresowe	Pomieszczenie
1.	Starostwo Powiatowe w Wyszkowie 07-200 Wyszków , Aleja Róż 2 Wydział Planowania Rozwoju i Wdrażania Programów Pomocowych	Pok. Nr 4,13
2.	Starostwo Powiatowe w Wyszkowie 07-200 Wyszków, Aleja Róż 2 Wydział Finansowy	Pok. Nr 11,12

STAROSTA

Bogdan Mirosław Pągowski

Załącznik nr 3
do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
u Beneficjenta PO KL

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 zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL oraz z Instrukcją Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL.

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

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 4

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 U Beneficjenta PO KL

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

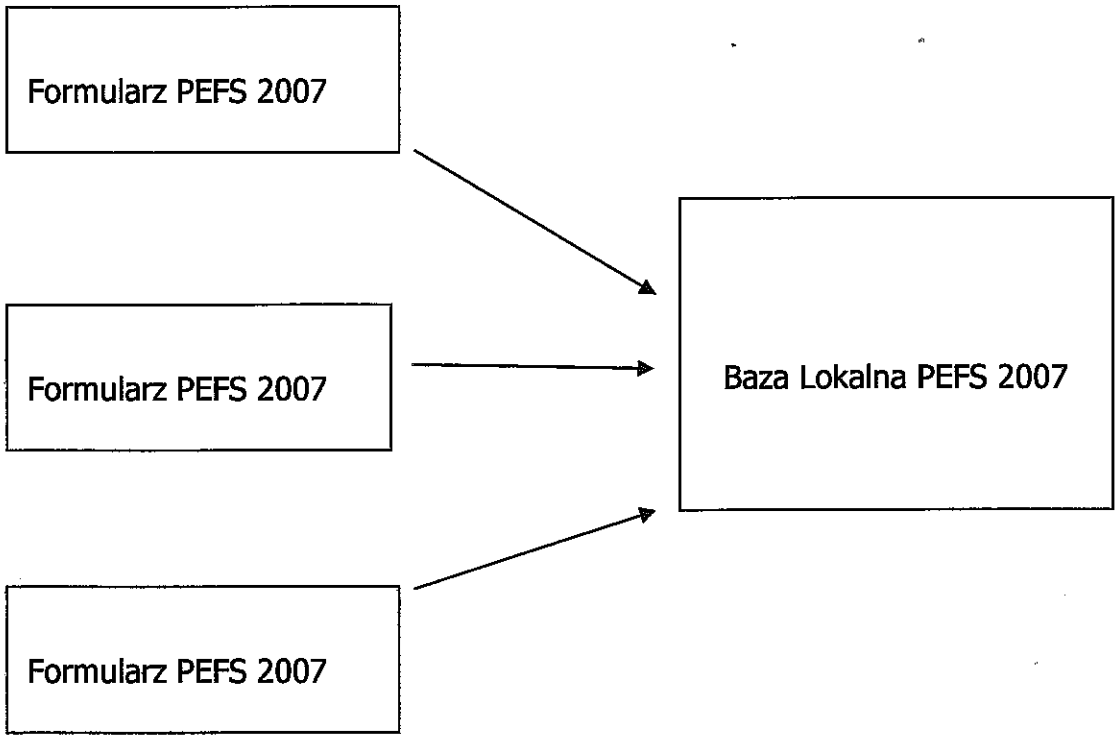
a) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
b) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy.
c) Monitory komputerów, na których są przetwarzane dane osobowe 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.

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 5

do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL

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.

STAROSTA
Bogdan Mirosław Pągowski

Załącznik nr 6
do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
u Beneficjenta PO KL

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

Tabela 1. Dane wspólne – powiązane z danymi osobowymi każdej osoby w zbiorze PEFS 2007

Lp.	Nazwa
1	Tytuł projektu (pole tekstowe)
2	Nr projektu (pole tekstowe)
3	Priorytet, w ramach którego realizowany jest projekt (pole słownikowe)
4	Działanie, w ramach którego realizowany jest projekt (pole słownikowe)
5	Poddziałanie, w ramach którego realizowany jest projekt (pole słownikowe)
6	Liczba osób niepełnosprawnych objętych wsparciem w ramach projektu (dane o charakterze statystycznym – pole liczbowe)
7	Liczba dzieci w wieku od 3 do 5 lat objętych wsparciem w ramach projektu (dane o charakterze statystycznym – pole liczbowe)

STAROSTA
Bogdan Mirosław Pągowski

CZĘŚĆ PIERWSZA:
DANE INSTYTUCJI OBJĘTYCH WSPARCIEM W RAMACH PROGRAMU, W TYM ICH PRACOWNIKÓW

Tabela 2. Dane instytucji, które otrzymują wsparcie w ramach EFS – powiązane z danymi z tabeli nr 1 i tabeli nr 5

	Lp.	Nazwa	Słownik
Dane podstawowe	1	Nazwa instytucji (pole tekstowe)	
	2	NIP (pole liczbowe)	
	3	REGON (pole liczbowe)	
	4	Typ instytucji (pole słownikowe)	Zgodnie z tabelą nr 3 – Typ instytucji
	5	Polska Klasyfikacja Działalności (PKD) (pole tekstowe)	
	6	Wielkość instytucji (pole słownikowe)	Mikroprzedsiębiorstwo
			Małe przedsiębiorstwo
			Średnie przedsiębiorstwo
			Duże przedsiębiorstwo
Dane teleadresowe	7	Ulica (pole tekstowe)	
	8	Nr budynku (pole tekstowe)	
	9	Nr lokalu (pole tekstowe)	
	10	Miejscowość (pole tekstowe)	
	11	Obszar (pole radiowe)	Obszar (teren) miejski
			Obszar (teren) wiejski
	12	Kod pocztowy (pole liczbowe)	
	13	Województwo (pole słownikowe)	

	14	Powiat (pole słownikowe)		
	15	Telefon kontaktowy (pole tekstowe)		
	16	Adres poczty elektronicznej (e-mail) (pole tekstowe)		
Szczegóły wsparcia	17	Rodzaj przyznanego wsparcia (pole słownikowe)	Zgodnie z Tabelą nr 4 – Rodzaj przyznanego instytucji wsparcia	
	18	Data rozpoczęcia udziału w projekcie (pole data)		
	19	Data zakończenia udziału w projekcie (pole data)		
	20	Czy wsparciem zostali objęci pracownicy instytucji (pole checkbox)	Nie	Tak *Zgodnie z Tabelą nr 5 – Dane uczestników projektów (pracowników instytucji), którzy otrzymują wsparcie w ramach EFS*
	21	Liczba osób objętych wsparciem w ramach instytucji (pole liczbowe)		

Tabela nr 3 – Typ instytucji

Priorytet	**TYP INSTYTUCJI**
1. Zatrudnienie i integracja społeczna	Instytucja rynku pracy, w tym: - Publiczne Służby Zatrudnienia Instytucja pomocy i integracji społecznej Służba więzienna Zakład poprawczy/schronisko dla nieletnich Przedsiębiorstwo

	Jednostka administracji rządowej Jednostka administracji samorządowej Organizacja pozarządowa Partnerzy społeczno-gospodarczy Inna
2. Rozwój zasobów ludzkich i potencjału adaptacyjnego przedsiębiorstw poprawa stanu zatrudnienia osób pracujących	Przedsiębiorstwo Instytucja świadcząca usługi na rzecz rozwoju przedsiębiorczości (np. członek KSU) Zakład Opieki Zdrowotnej Partnerzy społeczno-gospodarczy Uczelnia Instytucja naukowo badawcza Instytucja rynku pracy, w tym: - Publiczne Służby Zatrudnienia Jednostka administracji rządowej Jednostka administracji samorządowej Inna
3. Wysoka jakość systemu oświaty	Komisja egzaminacyjna Szkoła, w tym: - podstawowa - gimnazjalna - ponadgimnazjalna Przedszkole/inna forma edukacji przedszkolnej Placówka kształcenia ustawicznego/placówka kształcenia praktycznego/ośrodek dokształcania i doskonalenia zawodowego

	Zakład kształcenia i placówka doskonalenia nauczycieli Uczelnia, w tym: - publiczna - niepubliczna Jednostka naukowo badawcza Jednostka administracji rządowej, w tym - kuratorium oświaty Jednostka administracji samorządowej Inna
4. Szkolnictwo wyższe i nauka	Uczelnia Jednostka naukowo badawcza Jednostka administracji rządowej Państwowa Komisja Akredytacyjna Rada Główna Szkolnictwa Wyższego Inna
5. Dobre rządzenie	Jednostka administracji rządowej (w tym skarbowej), w tym: - ministerstwo/urząd centralny - urząd wojewódzki Jednostka administracji samorządowej - urząd marszałkowski - urząd powiatowy/urząd gminy Instytucja działająca na rzecz organizacji pozarządowych Instytucja dialogu społecznego Instytucja wymiaru sprawiedliwości

	KSAP Organizacja pozarządowa Partnerzy społeczni Inna
6. Rynek pracy otwarty dla wszystkich	Instytucja rynku pracy, w tym: - Publiczne Służby Zatrudnienia Organizacja pozarządowa Partnerzy społeczno-gospodarczy Inna
7.Promocja integracji społecznej	Instytucja pomocy społecznej Jednostka administracji samorządowej Organizacja pozarządowa Partnerzy społeczno-gospodarczy Inna
8. Regionalne kadry gospodarki	Przedsiębiorstwo Partnerzy społeczno-gospodarczy Organizacja pozarządowa Uczelnia Jednostka naukowo badawcza Instytucja wspierająca ekonomie społeczną Inna
9. Rozwój wykształcenia i kompetencji w regionach	Szkoła, w tym - podstawowa - gimnazjalna

	- ponad gimnazjalna Przedszkole/inna forma edukacji przedszkolnej Placówka kształcenia ustawicznego/placówka kształcenia praktycznego/ośrodek dokształcania i doskonalenia zawodowego Jednostka administracji samorządowej Inna

Tabela nr 4 – Rodzaj przyznanego instytucji wsparcia

Priorytet	**Rodzaj przyznanego wsparcia**
1. Zatrudnienie i integracja społeczna	Wdrożenie standardów usług Rozwój narzędzi i systemów informacyjnych Wypracowanie lub modyfikacja metod, usług i narzędzi programów rynku pracy Wdrożenie nowych rozwiązań w zakresie organizacji pracy Inne
2. Rozwój zasobów ludzkich i potencjału adaptacyjnego przedsiębiorstw poprawa stanu zatrudnienia osób pracujących	Usługi na rzecz przedsiębiorczości Uzyskanie akredytacji Centrum Monitorowania Jakości w Ochronie Zdrowia Rozwój standardów organizacyjnych Rozwój standardów usług Rozwój standardów kwalifikacji Inne
3. Wysoka jakość systemu oświaty	Wdrożenie systemu nadzoru pedagogicznego i oceny jakości pracy, szkoły Wsparcie systemu akredytacji Opracowanie i wdrożenie podstaw programowych, materiałów dydaktycznych, materiałów metodycznych, narzędzi diagnostycznych metod kształcenia w tym:

	- wdrożenie nowych form i zasad kształcenia nauczycieli Opracowanie i wdrożenie Krajowego Systemu Kwalifikacji Uruchomienie nowego typu studiów Opracowanie/usprawnienie systemów informatycznych Wsparcie systemu egzaminów zewnętrznych Inne
4. Szkolnictwo wyższe i nauka	Wdrożenie programu rozwojowego w tym: - nowe kierunki studiów - organizacja dodatkowych zajęć wyrównawczych dla studentów I roku kierunków matematyczni-przyrodniczych i technicznych - opracowanie programów i materiałów dydaktycznych - wdrożenie modelu zarządzania jakością i/lub kontroli jakości kształcenia Zamawianie kształcenia na kierunkach matematycznych, przyrodniczych i technicznych Inne
5. Dobre rządzenie	Wsparcie w zakresie poprawy standardów zarządzania Przygotowanie i wdrożenie wieloletniego planowania w tym: - planowania budżetowego w ujęciu zadaniowym Utworzenie i rozwój punktów obsługi interesantów oraz punktów informacyjnych Opracowanie i wdrożenie jednolitych standardów obsługi klienta Wprowadzenie systemu analizy potrzeb szkoleniowych Opracowanie standardów kompetencyjnych Tworzenie i wdrażanie programów rozwoju organizacji Wsparcie w zakresie wzmacniania potencjału regulacyjnego administracji publicznej Wdrożenie programu z zakresu bezpłatnego poradnictwa prawnego i

	obywatelskiego Wsparcie w zakresie budowania potencjału partnerów społecznych Inne
6. Rynek pracy otwarty dla wszystkich	Dofinansowanie zatrudnienia doradców zawodowych oraz pośredników pracy Doposażenie lub wyposażenie stanowiska pracy dla skierowanego bezrobotnego w ramach prac interwencyjnych Inne
7.Promocja integracji społecznej	Wsparcie finansowe dla utworzenia i/lub funkcjonowania instytucji Wzmocnienie kadrowe Inne
8. Regionalne kadry gospodarki	Wsparcie w zakresie skutecznego przewidywania i zarządzania zmianą Tworzenie i modernizacja programów outplacementu Doradztwo dla firmy Tworzenie, rozwój i aktualizacja Regionalnych Strategii Innowacji Inne
9. Rozwój wykształcenia i kompetencji w regionach	Wdrożenie programów rozwojowych szkół w tym: - wdrożenie programów rozwojowych we współpracy z przedsiębiorstwami Wsparcie dla istniejących i tworzenia nowych ośrodków przedszkolnych Wdrażanie programów i narzędzi efektywnego zarządzania placówką Wyposażenie w nowoczesne materiały dydaktyczne Inne

Tabela nr 5 – Dane uczestników projektów (pracowników instytucji), którzy otrzymują wsparcie w ramach EFS – powiązane z danymi z tabeli nr 1 oraz tabeli nr 2

	Lp.	Nazwa	Możliwe wartości
Dane uczestnika	1	Imię (imiona) (pole tekstowe)	
	2	Nazwisko (pole tekstowe)	
	3	Płeć (pole słownikowe)	Kobieta
			Mężczyzna
	4	Wiek w chwili przystępowania do projektu (pole liczbowe)	
	5	PESEL (pole liczbowe)	
	6	Nazwa instytucji (pole tekstowe)	
	7	Wykształcenie (pole słownikowe)	Brak
			Podstawowe
			Gimnazjalne
			Ponadgimnazjalne
			Pomaturalne
			Wyższe
	8	Opieka nad dziećmi do lat 7 lub opieka nad osobą zależną (pole checkbox)	Tak
			Nie
Dane kontaktowe	9	Ulica (pole tekstowe)	
	10	Nr domu *(pole tekstowe)*	
	11	Nr lokalu (pole tekstowe)	
	12	Miejscowość (pole tekstowe)	
	13	Obszar (pole radiowe)	Obszar (teren) miejski

			Obszar (teren) wiejski
	14	Kod pocztowy (pole liczbowe)	
	15	Województwo (pole słownikowe)	
	16	Powiat (pole słownikowe)	
	17	Telefon stacjonarny (pole tekstowe)	
	18	Telefon komórkowy (pole tekstowe)	
	19	Adres poczty elektronicznej (e-mail) (pole tekstowe)	
	20	Zatrudniony w (pole słownikowe)	mikroprzedsiębiorstwie
			małym przedsiębiorstwie
			średnim przedsiębiorstwie
			dużym przedsiębiorstwie
			administracji publicznej
			organizacji pozarządowej
	21	Rodzaj przyznanego wsparcia (pole słownikowe)	Zgodnie z Tabelą nr 4 – Rodzaj przyznanego wsparcia
	22	Wykorzystanie we wsparciu technik: e-learning/blended learning (pole	Tak

		checkbox)	Nie
	23	Data rozpoczęcia udziału w projekcie (pole data)	
	24	Data zakończenia udziału w projekcie (pole data)	
	25	Zakończenie udziału osoby we wsparciu zgodnie z zaplanowaną dla niej ścieżką uczestnictwa (pole checkbox)	Tak
			Nie

Tabela nr 6 - Rodzaj przyznanego wsparcia

Priorytet	**Rodzaj przyznanego wsparcia**
1. Zatrudnienie i integracja społeczna	Doradztwo Indywidualne Plany Działań Pomoc prawna Poradnictwo zawodowe Pośrednictwo pracy Staże/praktyki/przygotowanie zawodowe Studia I i (lub) II stopnia Studia podyplomowe Szkolenia/warsztaty/kursy Wizyty studyjne Zatrudnienie subsydiowane Inne
2. Rozwój zasobów ludzkich i potencjału adaptacyjnego przedsiębiorstw poprawa stanu zatrudnienia osób pracujących	Doradztwo Specjalizacje medyczne

	Studia podyplomowe Studia pomostowe Szkolenia/warsztaty/kursy Inne
3. Wysoka jakość systemu oświaty	Studia I i (lub) II stopnia Studia podyplomowe Staże/praktyki/przygotowanie zawodowe Zajęcia dodatkowe dla uczniów Szkolenia/warsztaty/kursy Inne
4. Szkolnictwo wyższe i nauka	Doradztwo Pośrednictwo pracy Staże/praktyki/przygotowanie zawodowe Studia doktoranckie Studia I i (lub) II stopnia Studia I i (lub) II stopnia zamawiane Studia podyplomowe Stypendia Szkolenia/warsztaty/kursy Zajęcia wyrównawcze dla studentów Inne
5. Dobre rządzenie	Doradztwo Staże/praktyki/przygotowanie zawodowe Studia podyplomowe

	Szkolenia/warsztaty/kursy Wizyty studyjne Inne
6. Rynek pracy otwarty dla wszystkich	Dofinansowanie kosztów dojazdów do miejsca pracy i zakwaterowania Doradztwo Indywidualne Plany Działań Poradnictwo zawodowe Pośrednictwo pracy Staże/praktyki/przygotowanie zawodowe Zatrudnienie subsydiowane Szkolenia/warsztaty/kursy Środki na rozwój przedsiębiorczości Wsparcie dla pracownika zatrudnionego w ramach projektu Wsparcie pomostowe Inne
7.Promocja integracji społecznej	Doradztwo Poradnictwo zawodowe Praca socjalna Staże/praktyki/przygotowanie zawodowe Szkolenia/warsztaty/kursy Zatrudnienie socjalne Zatrudnienie subsydiowane Inne
8. Regionalne kadry gospodarki	Doradztwo

	Staże/praktyki/przygotowanie zawodowe Stypendia Szkolenia/warsztaty/kursy Inne
9. Rozwój wykształcenia i kompetencji w regionach	Doradztwo Staże/praktyki/przygotowanie zawodowe Studia I i (lub) II stopnia Studia podyplomowe Stypendia Szkolenia/warsztaty/kursy Zajęcia dodatkowe dla uczniów Inne

STAROSTA
Bogdan Mirosław Pągowski

CZĘŚĆ DRUGA:

DANE OSÓB OBJĘTYCH WSPARCIEM, JAKO NIEPRACUJĄCE ORAZ PRACUJĄCE, KTÓRE UCZESTNICZĄ WE WSPARCIU Z WŁASNEJ INICJATYWY

Tabela nr 7 - Dane uczestników projektów, którzy otrzymują wsparcie w ramach EFS – powiązane z danymi z tabeli nr 1

	Lp.	Nazwa	Możliwe wartości
Dane uczestnika	1	Imię (imiona) (pole tekstowe)	
	2	Nazwisko (pole tekstowe)	
	3	Płeć (pole słownikowe)	Kobieta
			Mężczyzna
	4	Wiek w chwili przystępowania do projektu (pole liczbowe)	
	5	PESEL (pole liczbowe)	
	6	Wykształcenie (pole słownikowe)	Brak
			Podstawowe
			Gimnazjalne
			Ponadgimnazjalne
			Pomaturalne

				Wyższe
	7	Opieka nad dziećmi do lat 7 lub opieka nad osobą zależną (pole checkbox)		Tak
				Nie
Dane kontaktowe	8	Ulica (pole tekstowe).		
	9	Nr domu (pole tekstowe)		
	10	Nr lokalu (pole tekstowe)		
	11	Miejscowość (pole tekstowe)		
	12	Obszar (pole radiowe)		Obszar (teren) miejski
				Obszar (teren) wiejski
	13	Kod pocztowy (pole liczbowe)		
	14	Województwo (pole słownikowe)		
	15	Powiat (pole słownikowe)		
	16	Telefon stacjonarny (pole tekstowe)		
	17	Telefon komórkowy (pole tekstowe)		
	18	Adres poczty elektronicznej (e-mail) (pole tekstowe)		
Dane dodatkowe	19	Status osoby na rynku pracy w chwili przystąpienia do projektu (pole słownikowe)	Bezrobotny	Tak
				Nie
			w tym	Osoba długotrwale bezrobotna

			Nieaktywny zawodowo	Tak
				Nie
			w tym	Osoba ucząca się lub kształcąca
			Zatrudniony	Tak
				Nie
			w tym	Rolnik
				Samozatrudniony
				Zatrudniony w mikroprzedsiębiorstwie
				Zatrudniony w małym przedsiębiorstwie
				Zatrudniony w średnim przedsiębiorstwie
				Zatrudniony w dużym przedsiębiorstwie
				Zatrudniony w administracji publicznej
				Zatrudniony w organizacji pozarządowej
	20	Rodzaj przyznanego wsparcia (pole słownikowe)		Zgodnie z tabelą 8 – Rodzaj przyznanego wsparcia
	21	Wykorzystanie we wsparciu technik: e-learning/blended learning (pole checkbox)		Tak
				Nie
	22	Data rozpoczęcia udziału w projekcie (pole data)		
	23	Data zakończenia udziału w projekcie (pole data)		

	24	Zakończenie udziału osoby we wsparciu zgodnie z zaplanowaną dla niej ścieżką uczestnictwa (pole checkbox)	Tak
			Nie
	25	Powód wycofania się z proponowanej formy wsparcia (pole słownikowe)	Podjęcie zatrudnienia
			Podjęcie nauki
			Inne

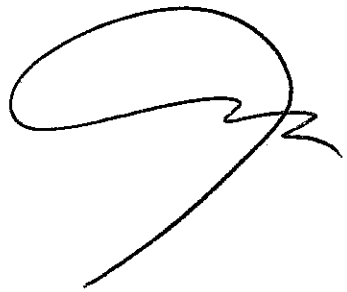
Tabela nr 8 – Rodzaj przyznanego wsparcia

Priorytet	**Rodzaj przyznanego wsparcia**
1. Zatrudnienie i integracja społeczna	Doradztwo Indywidualne Plany Działań Pomoc prawna Poradnictwo zawodowe Pośrednictwo pracy Staże/praktyki/przygotowanie zawodowe Studia I i (lub) II stopnia Studia podyplomowe Szkolenia/warsztaty/kursy Wizyty studyjne Zatrudnienie subsydiowane Inne
2. Rozwój zasobów ludzkich i potencjału adaptacyjnego przedsiębiorstw poprawa stanu zatrudnienia osób pracujących	Doradztwo Specjalizacje medyczne Studia podyplomowe

	Studia pomostowe Szkolenia/warsztaty/kursy Inne
3. Wysoka jakość systemu oświaty	Studia I i (lub) II stopnia Studia podyplomowe Staże/praktyki/przygotowanie zawodowe Zajęcia dodatkowe dla uczniów Szkolenia/warsztaty/kursy Inne
4. Szkolnictwo wyższe i nauka	Doradztwo Pośrednictwo pracy Staże/praktyki/przygotowanie zawodowe Studia doktoranckie Studia I i (lub) II stopnia Studia I i (lub) II stopnia zamawiane Studia podyplomowe Stypendia Szkolenia/warsztaty/kursy Zajęcia wyrównawcze dla studentów Inne
5. Dobre rządzenie	Doradztwo Staże/praktyki/przygotowanie zawodowe Studia podyplomowe Szkolenia/warsztaty/kursy

	Wizyty studyjne Inne
6. Rynek pracy otwarty dla wszystkich	Dofinansowanie kosztów dojazdów do miejsca pracy i zakwaterowania Doradztwo Indywidualne Plany Działań Poradnictwo zawodowe Pośrednictwo pracy Staże/praktyki/przygotowanie zawodowe Zatrudnienie subsydiowane Szkolenia/warsztaty/kursy Środki na rozwój przedsiębiorczości Wsparcie dla pracownika zatrudnionego w ramach projektu Wsparcie pomostowe Inne
7.Promocja integracji społecznej	Doradztwo Poradnictwo zawodowe Praca socjalna Staże/praktyki/przygotowanie zawodowe Szkolenia/warsztaty/kursy Zatrudnienie socjalne Zatrudnienie subsydiowane Inne
8. Regionalne kadry gospodarki	Doradztwo Staże/praktyki/przygotowanie zawodowe

	Stypendia Szkolenia/warsztaty/kursy Inne
9. Rozwój wykształcenia i kompetencji w regionach	Doradztwo Staże/praktyki/przygotowanie zawodowe Studia I i (lub) II stopnia Studia podyplomowe Stypendia Szkolenia/warsztaty/kursy Zajęcia dodatkowe dla uczniów Inne



Załącznik nr 7
do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL

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

STAROSTA
Bogdan Mirosław Pągowski

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM DLA SYSTEMU PODSYSTEM MONITOROWANIA EUROPEJSKIEGO FUNDUSZU 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 Starostwie Powiatowym w Wyszkowie zwanym/ej dalej „Beneficjentem".

§ 2.

Użyte w Instrukcji określenia oznaczają:

1) Administrator Danych	- Starosta Powiatu;
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 nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 u Beneficjenta;
5) Administrator Systemu u Beneficjenta	- osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń PEFS 2007 u Beneficjenta, o ile zadanie te zostały wyłączone z zakresu kompetencji Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta i powierzone przez osobę upoważnioną do podejmowania decyzji u Beneficjenta innemu pracownikowi;
5) naruszenie zabezpieczenia PEFS 2007	- jakiekolwiek 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.

1. Osobą odpowiedzialną za przydział identyfikatorów i pierwszych haseł dla użytkowników u Beneficjenta jest Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta. 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 Bezpieczeństwa dla zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta.

4. Jakakolwiek zmianą 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. 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 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 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 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, o której mowa w § 29 pkt 1 ustawy o ochronie danych osobowych, tzn. 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 przepisy o ochronie danych osobowych.

§ 33.

Instrukcja nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia PEFS 2007.

STAROSTA
Bogdan Mirosław Pągowski