Załącznik do zarządzenia Nr 115/2009
Kierownika Ośrodka Pomocy Społecznej
Gminy Lubawa z dnia 2 lutego 2009r.

Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa.

Opracowali :

Administrator Bezpieczeństwa Informacji
Referent Ośrodka Pomocy Społecznej Gminy Lubawa
Marcin Kulkowski

Zastępca Administratora Bezpieczeństwa Informacji
Referent Ośrodka Pomocy Społecznej Gminy Lubawa
Lucyna Gacioch

Spis treści

Wykaz załączników

WPROWADZENIE

Dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Ośrodku Pomocy Społecznej Gminy Lubawa.

Opisane zasady określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych stosowanych w Ośrodku Pomocy Społecznej Gminy Lubawa.

Dokument zwraca uwagę na konsekwencje, jakie mogą ponieść osoby przekraczające określone granice oraz procedury postępowania w celu zapobiegania i minimalizowania skutków zagrożeń.

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

Dokument „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa", zwany dalej „Polityką bezpieczeństwa", wskazuje 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 § 4 rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz. 1433) 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:
    a. stwierdzono naruszenie zabezpieczenia systemu informatycznego,
    b. stan urządzeń, zawartość zbiorów danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci Ośrodka Pomocy Społecznej Gminy Lubawa mogą wskazywać na naruszenie zabezpieczeń tych danych.

2. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Ośrodka.

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.

4. Administratorem danych jest Kierownik Ośrodka Pomocy Społecznej Gminy Lubawa, jego obowiązki określa załącznik nr 1.

5. Administrator danych wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Ośrodka, zwanego dalej Administratorem Bezpieczeństwa oraz zastępcę Administratora Bezpieczeństwa Informacji.

6. Administrator bezpieczeństwa realizuje zadania w zakresie ochrony danych, a w szczególności:
   I. ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Ośrodka,
   II. podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do baz danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   III. niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   IV. nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

7. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.

8 . Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.),
2) rozporządzeniem 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. z 2004 r. Nr 100, poz.1024),
3) ustawą z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005r. Nr 64, poz. 565)
4) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. NR 11, poz. 95 z późn. zm.),
5) rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 177 poz. 1433).

1. Opis zdarzeń naruszających ochronę danych osobowych

1.1. Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, zalania, ogień, przerwy w zasilaniu w energię elektryczną, zwarcia i przepięcia w sieci elektroenergetycznej). Ich występowanie może prowadzić do utraty integralności danych, ich uszkodzenia, zniszczenia, uszkodzenia systemów komputerowych oraz elementów technicznych komputera lub sieci. Ciągłość systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych,
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, działanie wirusów). Może dojść do zniszczenia danych, zakłócenia ciągłości pracy systemu lub naruszenia 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 składników technicznych systemu.

1.2. Przypadki naruszenia ochrony danych osobowych

Przypadki zakwalifikowane jako naruszenie 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.: 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) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzenie próby modyfikacji danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

8) niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawnienie osobom nieupoważnionym danych osobowych, objętych tajemnicą procedur ochrony przetwarzania lub innych strzeżonych elementów zabezpieczeń systemu,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy, co świadczy o przełamaniu lub zaniechaniu ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu do sieci lub komputera, itp.,
11) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. "luk w systemie", itp.,
12) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia oraz skasowanie lub skopiowanie w sposób niedozwolony danych osobowych,
13) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie z programu, systemu przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

1.3. Inne przypadki

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. papier (wydruki), dyskietki w formie niezabezpieczonej itp.

2. Zabezpieczenie danych osobowych

2.1. Środki techniczne

Do zastosowanych środków technicznych należą:

1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
2) pomieszczenia, w których stoi serwer i komputery zawierające dane osobowe i kartoteki osobowe są zabezpieczone poprzez okratowane okna oraz system alarmowy.
3) do pomieszczeń, w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami. Dostęp do pomieszczenia z serwerami jest zabezpieczony przez wzmocnione drzwi zamykanych na zamek,
4) szczególne zabezpieczenie centrum przetwarzania danych (serwer) poprzez zastosowanie dostępu do pomieszczenia tylko osobom upoważnionym (Administrator

Bezpieczeństwa i jego zastępca) bądź osobom nieupoważnionym w obecności administratora bezpieczeństwa lub jego zastępcy.

2.2. Zabezpieczenia danych w systemie informatycznym

Wprowadza się następujące zabezpieczenia danych w systemie informatycznym:

1. Na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się **wysoki** poziom zabezpieczeń.
2. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera, na którym znajdują się bazy danych zapewnia zasilacz UPS APC 1000VA oraz uziemiona szafa rack-owa 19', w której znajduje się serwer.
3. Zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji. Nieudane próby logowania są rejestrowane. 5 nieudanych prób logowania powoduje czasową blokadę konta użytkownika (30 minut). Blokadę konta może usunąć tylko Administrator Bezpieczeństwa. Logowanie do systemu możliwe jest tylko w godzinach pracy Ośrodka.
4. Składnia hasła musi składać się z co najmniej 5 znaków oraz zawierać znaki specjalne, cyfry, duże i małe litery. Hasło jest ważne 30 dni. System monituje o jego zmianę 10 dni przed jego wygaśnięciem.
5. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
6. Administrator Bezpieczeństwa ma uprawnienia do definiowania kont użytkowników i haseł.
7. Wykorzystany jest system szyfrowania danych przesyłanych wewnątrz sieci oraz protokół Kerberos uniemożliwiający odczyt danych osobom nieupoważnionym.
8. W celu ochrony przed dostępem do baz danych i komputerów z sieci publicznej (Internet) wykorzystuje się system zapory ogniowej oraz system zasad dostępu zaimplementowany w routerze - I stopień filtracji. Firewall zawarty w systemach operacyjnych Windows XP stosowanych w Ośrodku jest II stopniem filtracji. W przypadku naruszenia zasad bezpieczeństwa router (bramka internetowa) natychmiast odcina wszystkie połączenia na porcie WAN do czasu ich odblokowania przez Administratora Bezpieczeństwa.
9. Podłączenie się do wewnętrznej sieci Ośrodka komputera nieuprawnionego spowoduje natychmiastowe zarejestrowanie tego faktu w logach serwera oraz routera. Komputer ten nie będzie miał uprawnień do korzystania z zasobów sieciowych Ośrodka kontrolowanych przez protokół Kerberos.
10. Zastosowano kilkustopniowe uwierzytelnianie komputera w sieci lokalnej Ośrodka poprzez.
    - identyfikację na podstawie unikalnego adresu MAC
    - statyczne przydzielenie numeru IP przez serwer DHCP (w ograniczonym zakresie danej klasy numerów IP)

- jednoznaczną identyfikację po nazwie DNS w lokalnej domenie Ośrodka
- określenie mu praw dostępu do poszczególnych zasobów.

11. Porty protokołów udp i tcp są pozamykane, a korzystanie z poszczególnych usług sieciowych mają tylko hosty z góry zdefiniowane przez Administratora Bezpieczeństwa.
12. Wysyłanie wszelkich informacji z sieci lokalnej Ośrodka ograniczone jest do minimum, odbywa się tylko w godzinach pracy Ośrodka, bądź za zgodą Administratora Bezpieczeństwa w ustalonych z pracownikiem nadgodzinach i dniach wolnych od pracy.
13. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe. Aktualizacje dokonują się automatycznie w cyklu pracy systemu operacyjnego.
14. Komputery podpięte są do wspólnej bazy aktualizacji na serwerze dzięki czemu docierają do nich tylko aktualizacje sprawdzone i zatwierdzone przez Administratora Bezpieczeństwa.
15. Kopie bezpieczeństwa na nośnikach DVD wykonuje okresowo Administrator Bezpieczeństwa. Kopie bezpieczeństwa przechowywane są w szafie zamykanej zamkiem meblowym. Dostęp do nośników zawierających kopie danych ma tylko Administrator Bezpieczeństwa.
16. Kartoteki papierowe znajdują się w meblowych szafach, zamykanych na zamki meblowe w pokojach, w których przetwarzane są dane osobowe.
17. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
18. Stosuje się następujące zabezpieczenia organizacyjne przed dostępem do danych osób niepowołanych:
    a) dostęp do danych mają wyłącznie pracownicy wyznaczeni przez Administratora Danych. Administrator Danych prowadzi ścisły rejestr tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych, łącznie z ich identyfikatorami w systemie.
    b) w pokoju, do którego dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie,
    c) w przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacze ekranu.

2.3. Środki organizacyjne

Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

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) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

2.4. Zabezpieczenia przed utrata danych

W celu ochrony przed utratą danych w Ośrodku stosowane są następujące zabezpieczenia:

1) odrębna sieć zasilająca sprzęt komputerowy (wydzielone obwody),
2) ochrona serwera przed zanikiem zasilania poprzez stosowanie zasilacza UPS,
3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na nośnikach CD, DVD i macierzy dyskowej, z których w przypadku awarii odtwarzane są dane i system operacyjny.

Opis struktur zbiorów danych przetwarzanych w Ośrodku określa załącznik nr 2.

2.5. Zbiory danych osobowych

Wykaz zbiorów danych osobowych, systemów informatycznych zastosowanych do ich przetwarzania oraz pomieszczeń w których przetwarzane są dane osobowe w Ośrodku Pomocy Społecznej Gminy Lubawa przedstawia załącznik nr 3.

3. Kontrola przestrzegania zasad zabezpieczenia danych osobowych

3.1. Nadzór ABI

Administrator Bezpieczeństwa sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w „Polityce Bezpieczeństwa".

3.2. Kontrola logów systemowych

Administrator Bezpieczeństwa co najmniej raz w tygodniu sprawdza logi systemowe serwerów, routerów i pozostałych urządzeń aktywnych w sieci, wykluczając bądź stwierdzając naruszenie Polityki Bezpieczeństwa.

3.3. Obowiązki ABI

Szczegółowe obowiązki Administratora Bezpieczeństwa określa załącznik nr 4.

4. Postępowanie w przypadku naruszenia ochrony danych osobowych

4.1. Przypadki stwierdzenia naruszenia ochrony danych osobowych

Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa lub jego zastępcę w przypadku stwierdzenia naruszenia:

- zabezpieczenia systemu informatycznego,
- technicznego stanu urządzeń,
- zawartości zbioru danych osobowych,
- ujawnienia metody pracy lub sposobu działania programu,
- jakości transmisji danych w sieciach komputerowych mogącej wskazywać na naruszenie zabezpieczeń tych danych,
- innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie pomieszczeń, pożar, itp.).

W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub jego zastępcy należy powiadomić Administratora Danych (Kierownika Ośrodka).

4.2. Czynności podejmowane do czasu przybycia ABI na miejsce naruszenia ochrony danych osobowych

Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa, 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,
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.

4.3. Czynności podejmowane przez ABI lub jego zastępcę po przybyciu na miejsce naruszenia ochrony danych osobowych

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Ośrodka,
2) żąda dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym zdarzeniem naruszenia ochrony danych,
3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych. Jeżeli taka potrzeba istnieje, nawiązuje kontakt ze specjalistami.

4.4. Raport z naruszenia bezpieczeństwa ochrony danych osobowych

Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 5, który powinien zawierać w szczególności:

1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu, 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.

Raport, o którym mowa w ust. 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych (Kierownikowi Ośrodka), a w przypadku jego nieobecności osobie uprawnionej.

Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii bezpieczeństwa oraz określa termin wznowienia przetwarzania danych (jeśli jest to możliwe).

Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Ośrodka i Administratora Bezpieczeństwa.

Analiza, o której mowa w ust. 8, 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.

5. 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, bądź też nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, upoważnionych do przetwarzania danych osobowych, zgodnie z załącznikiem nr 6.

3. Osoby uprawnione do przetwarzania danych osobowych obowiązuje zakres obowiązków, które stanowi załącznik nr 7.

4. Osoby uprawnione do przetwarzania danych osobowych składają oświadczenia zgodnie z załącznikiem nr 8.

5. Osoby uprawnione do przetwarzania danych osobowych otrzymują Upoważnienie do przetwarzania danych osobowych zgromadzonych w zbiorze danych osobowych wydane przez Administratora Danych Osobowych (Kierownika Ośrodka) zgodnie z załącznikiem nr 9.

6. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, upoważnionych do przetwarzania danych osobowych Beneficjentów Ostatecznych (uczestników) projektów w ramach Programu Operacyjnego Kapitał Ludzki 2007-2013 współfinansowanych przez Unię Europejska w ramach Europejskiego Funduszu Społecznego, zgodnie z załącznikiem nr 10.

7. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić Kartę Uprawnień dostępu użytkowników do formularza PEFS 2007 w zakresie POKL, zgodnie z załącznikiem nr 11.

8. Osoby uprawnione do przetwarzania danych osobowych Beneficjentów Ostatecznych (uczestników) projektów w ramach Programu Operacyjnego Kapitał Ludzki 2007-2013 współfinansowanych przez Unię Europejska w ramach Europejskiego Funduszu Społecznego otrzymują

    A. odrębne upoważnienie, zgodnie z załącznikiem nr 12,
    B. upoważnienie dostępu do formularza PEFS 2007 w zakresie POKL, zgodnie z załącznikiem nr 13.

9. 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.

10. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

11. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity 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).