Załącznik nr 1
do Zarządzenia Nr 6/2011
Kierownika Ośrodka Pomocy Społecznej
w Trzcińsku-Zdroju
z dnia 2. lutego 2011 roku

Polityka bezpieczeństwa

i instrukcja zarządzania systemem informatycznym

służącym do przetwarzania danych osobowych

w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju

Trzcińsko-Zdrój, grudzień 2010 r.

Spis treści

WPROWADZENIE

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101, z 2002 r., poz. 926),
2) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. Nr 11, poz. 95 z późn. zm.),
3) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),

Niniejszy dokument reguluje sprawy ochrony danych osobowych zawartych w systemie informatycznym eksploatowanym w lokalnej sieci komputerowej oraz zbiorów danych zapisanych w postaci dokumentacji papierowej w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju.

Ilekroć w dokumencie jest mowa o:
„OPS" – należy przez to rozumieć Ośrodek Pomocy Społecznej w Trzcińsku-Zdroju
„Kierowniku" – należy przez to rozumieć Kierownika Ośrodka Pomocy Społecznej w Trzcińsku-Zdroju
„Administratorze Bezpieczeństwa" – należy przez to rozumieć Administratora Bezpieczeństwa Ośrodka Pomocy Społecznej w Trzcińsku-Zdroju.
„Polityce bezpieczeństwa"- należy przez to rozumieć dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju".

Instrukcja dotyczy następujących niżej wymienionych baz danych:

1. Pomoc społeczna,
2. Fundusz Alimentacyjny
3. Świadczenia rodzinne
4. Kadry i płace

oraz zbiór danych:

5. Klub Integracji Społecznej

W OPS w Trzcińsku-Zdroju przetwarza się również dane w bazie danych „Dodatki mieszkaniowe" na podstawie umowy powierzenia danych z Urzędu Miejskiego w Trzcińsku-Zdroju.

Do przetwarzania zbiorów danych zawierających dane osobowe stosuje się następujące programy:

Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innym jednostkom budżetowym Gminy na podstawie przepisów ustawy o ochronie danych osobowych. Za ochronę danych osobowych, których przetwarzanie zostało powierzone innym jednostkom budżetowym Gminy Trzcińsko-Zdrój odpowiadają kierownicy tych jednostek.

Opis struktur zbiorów danych jest zawarty w Załączniku Nr 5 do niniejszego dokumentu. Granice obszarów, w których przetwarzane są dane osobowe zostały opisane w Załączniku Nr 6. Administrator Danych Osobowych w wyjątkowych sytuacjach może zarządzić zmianę obszarów przetwarzania danych osobowych,.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych pracujących w OPS. 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", wskazujący sposób zabezpieczenia systemów informatycznych 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 póz. 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:
   - stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   - 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 OPS a także innych pracowników zatrudnionych w ramach stażu lub przygotowania zawodowego.
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 systemie informatycznym OPS.
4. Administrator Danych, którym jest Kierownik OPS, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych OPS, zwanego dalej „Administratorem Bezpieczeństwa" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa" (jeśli jest to konieczne ze względu na ilość obowiązków oraz konieczność ustalenia zastępstw na czas nieobecności.
5. „Administrator bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:
   - ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych OPS,

- 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,
- niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
- nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.
7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

Rozdział 1

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:
   - zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu; ciągłość pracy systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   - zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   - 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. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   - 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.,
   - niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   - 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 fakt pozostawienia serwisantów bez nadzoru,
   - pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   - jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   - naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   - stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   - nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
   - ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
   - 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.,

- ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki”, itp.,
- podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- 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, płytach DVD lub innych nośnikach itp.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

§ 1.
Cele i zasady ogólne

1. Administratorem danych osobowych zawartych i przetwarzanych w systemie informatycznym Ośrodka Pomocy Społecznej jest Kierownik Ośrodka Pomocy Społecznej w Trzcińsku-Zdroju.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych OPS, a w szczególności:
   - zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   - zapobiegać zabraniu danych przez osobę nieuprawnioną,
   - zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych. Szczegółowe obowiązki Administratora Danych zawarte są w Załączniku Nr 1.

§ 2.
Cele ochrony i zasady ogólne

1. Celem wprowadzonych niniejszą Polityką zabezpieczeń i obostrzeń jest ochrona danych osobowych zawartych w eksploatowanym w sieci komputerowej LAN systemie.
   Określone niżej sposoby zabezpieczeń dotyczą:
   1.1 zabezpieczeń przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu tj. wprowadzanie danych, aktualizacji lub usuwania danych, wyświetlania lub drukowania zestawień,
   1.2 ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych.
   1.3 systemu zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia oraz sposobów dostępu do tych pomieszczeń pracowników, personelu pomocniczego Urzędu oraz serwisu zewnętrznego,
   1.4 monitorowania systemu zabezpieczeń,
   1.5 zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych.

2. Strategia ochrony danych osobowych opiera się na następujących zasadach:
   2.1 fizyczny dostęp do pomieszczeń, w których eksploatowane są systemy informatyczne blokują drzwi i systemy alarmowe.
   2.2 podstawowym sposobem zabezpieczenia danych i dostępu do nich jest system definiowania użytkowników, grup użytkowników oraz haseł. Są to zabezpieczenia programowe wmontowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym.
   2.3 dodatkowym systemem zabezpieczenia jest stosowanie kryptograficznej ochrony danych, jeśli taką funkcję oferuje system operacyjny.
   2.4 dodatkowe kopie danych zarchiwizowanych na nośnikach magnetycznych lub płytach CD lub DVD są przechowywane w oddzielnym budynku – chronią w ten sposób

dane na wypadek pożaru, klęski żywiołowej lub katastrofy. Prowadzona jest ścisła ewidencja tych nośników,

2.5 w pomieszczeniach, w których zainstalowany jest serwer i komputery zawierające bazy danych jest zainstalowany system alarmowy i przeciwpożarowy,

2.6 zagadnienia związane z ochrona danych i obowiązki stąd wynikające są ujęte w zakresach czynności pracowników stanowiące Załącznik Nr 3,

2.7 każdy pracownik OPS podpisze oświadczenie stanowiące Załącznik Nr 4,

2.8 za całość polityki bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji.

§ 3.
Zabezpieczenia

Wprowadza się następujące zabezpieczenia danych w systemie informatycznym:

1. Na wszystkich stacja roboczych, na których przetwarzane są dane osobowe wprowadza się **wysoki** poziom zabezpieczeń.
2. Pomieszczenia, w których znajduje się sprzęt komputerowy, zawierający dane osobowe i kartoteki osobowe są zabezpieczone poprzez okratowane okna oraz system alarmowy i przeciwpożarowy. Wykaz tych pomieszczeń zawiera Załącznik Nr 6.
3. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
4. Uruchomienie stacji roboczych, na których przetwarzane są dane osobowe wymaga podania hasła BIOS-u,
5. Zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji.
6. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
7. Administrator Bezpieczeństwa Informacji ma uprawnienia do definiowania kont użytkowników i haseł.
8. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się system zapory ogniowej dostępnej w systemie operacyjnym lub w programie antywirusowym i antywłamaniowym.
9. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe. Aktualizacja bazy wirusów wykonywana jest automatycznie.
10. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
11. Kopie bezpieczeństwa na nośnikach magnetycznych wykonują okresowo pracownicy w ramach swoich obowiązków. Kopie bezpieczeństwa przechowywane są w kasie pancernej w pomieszczeniu Kasy Urzędu Miejskiego. Zapasowe kopie bezpieczeństwa są przechowywane w innym budynku – wyznaczonym przez Administratora Danych Osobowych - również w szafie pancernej. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.
12. Kartoteki papierowe znajdują się w pokojach, w których przetwarzane dane osobowe i są zamknięte w meblowych szafach, zamykanych na zamki meblowe.
13. 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. wygaszacie ekranu, których deaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.
   d) częstotliwość tworzenia kopii bezpieczeństwa określa instrukcja archiwowania zasobów. Za wykonanie tych kopii odpowiedzialne są osoby przetwarzające dane osobowe. Kopie te są wykonywane na nośnikach optycznych (płyty CD-R/CD-RW, DVD) przynajmniej raz na miesiąc.

14. Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Danych Osobowych może zarządzić zastosowanie dodatkowych zabezpieczeń, mających na celu podwyższenie stopnia bezpieczeństwa przetwarzanych danych osobowych.

§ 4.
Monitorowanie zabezpieczeń

1. Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:
   a) Administrator Danych
   b) Administrator Bezpieczeństwa Informacji
2. W ramach monitoringu należy przeprowadzać następujące działania:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
   b) kontrola ewidencji nośników magnetycznych i optycznych,
   c) sprawdzania częstotliwości zmian haseł,
3. Administrator Bezpieczeństwa sporządza roczne plany kontroli zatwierdzone przez Administratora Danych i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
4. Na podstawie zgromadzonych materiałów, o których mowa w pkt. 3. Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi Danych Osobowych.

§ 5.
Szkolenia

1. Szkolenie podstawowe dotyczące bezpieczeństwa danych obejmuje wszystkich pracowników OPS.
2. System szkoleń szczegółowych obejmuje pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych, w tym danych osobowych.
3. Tematyka szkoleń obejmuje:
   a) Przepisy i instrukcje wewnętrzne dotyczące ochrony danych archiwizacji zasobów i przechowywania nośników, niszczenie wydruków i zapisów na nośnikach magnetycznych i optycznych,
   b) Zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochroną systemów na poszczególnych stanowiskach.

§ 6.
Archiwizowanie danych

1. Dane programów kopiowane są w trybie miesięcznym. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane osobowe lub administrator bezpieczeństwa.
2. Nośniki z kopiami bezpieczeństwa przekazywane są do pomieszczenia Kasy w budynku Urzędu Miejskiego w Trzcińsku-Zdroju.
3. Dyskietki, na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, aby nie można było odtworzyć ich zawartości. Płyty CD, na których przechowuje się kopie awaryjne niszczy się trwale w sposób mechaniczny.
4. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza Administrator Bezpieczeństwa.
5. W przypadku stwierdzenia uszkodzenia nośnika, Administrator Bezpieczeństwa sporządza protokół zniszczenia tego nośnika, potwierdzony przez pracownika odpowiedzialnego za przetwarzanie danych osobowych, które znajdowały się na tym nośniku.

§ 7.
Niszczenie wydruków i zapisów na nośnikach magnetycznych

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
2. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa.
3. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać itp.).
4. Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone przez spalenie w piecu c. o. lub zniszczone w niszczarce.

Rozdział 3

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik Ośrodka, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informację o mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi Bezpieczeństwa Informacji.

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:
   - 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,
   - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   - zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   - podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   - podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
   - zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   - udokumentować wstępnie zaistniałe naruszenie,
   - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

4 Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:
   - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Ośrodka,
   - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   - rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych Osobowych,
   - nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami z jednostki nadrzędnej (Urząd Miejski) lub pracownikami z firm specjalistycznych.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego Załącznik Nr 7**,** który powinien zawierać w szczególności:

- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
- określenie czasu i miejsca naruszenia i powiadomienia,
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w pkt. 5, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych Osobowych, a w przypadku jego nieobecności osobie uprawnionej.

7. 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 zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez kierownictwo OPS tj. Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji. W przypadkach uzasadnionych w zespole mogą uczestniczyć pracownicy jednostki nadrzędnej (Urzędu Miejskiego, Administrator Bezpieczeństwa Informacji, Pełnomocnik ds. Ochrony Informacji Niejawnych).

9. Analiza, o której mowa w ust. 9, 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 4

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 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 8 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 Danych Osobowych.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Danych Osobowych 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, póz. 926) 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 (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).

6. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju” wchodzi w życie z dniem jej podpisania przez Kierownika OPS.

Załącznik Nr 1 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju”

Obowiązki Administratora Danych

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów,
   c) merytorycznie poprawne i adekwatne w stosunku do celów.
2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
5. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
7. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8. Odpowiada za to, by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:
   a) ochronę danych przed niepowołanym dostępem,
   b) nieuzasadnioną modyfikację lub zniszczenie danych,
   c) nielegalne ujawnienie danych.

   w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.
9. Rejestruje zbiory danych osobowych w Biurze Generalnego Inspektora Ochrony Danych Osobowych.
10. Rejestruje nowe zbiory danych osobowych w Biurze Generalnego Inspektora Ochrony Danych Osobowych.

Załącznik Nr 2 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju”

Obowiązki Administratora Bezpieczeństwa Informacji

1. Nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.
2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.
3. Nadzór na wykorzystywany w OPS oprogramowaniem oraz jego legalnością.
4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe,
5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.
6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.
7. Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.
8. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
9. Definiowanie użytkowników i haseł dostępu.
10. Przeprowadzanie symulowanych włamań do systemu w celu ustalenia aktualnego poziomu zabezpieczeń.
11. Aktualizowanie oprogramowania antywirusowego i innego chyba, że aktualizacje te wykonywane są automatycznie.
12. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
13. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.
14. Sporządzanie planów kontroli zatwierdzanych przez Administratora Danych oraz przeprowadzanie zgodnie z nimi kontroli.
15. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Załącznik Nr 3 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju”

Dodatkowy zakres obowiązków dla pracowników Ośrodka Pomocy Społecznej o w Trzcińsku-Zdroju

1. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w Urzędzie Polityką Bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m. in.:
   a) Chronić dane przed dostępem osób nieupoważnionych,
   b) Chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
   c) Chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
   d) Utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w OPS.
   e) Archiwizować dane zgodnie z instrukcją technologiczną,
   f) Prowadzić niezbędną, przewidzianą instrukcją technologiczną dokumentację pracy z systemem, archiwizowania danych itp.
2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
   a) ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach,
   b) kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną kopiami bezpieczeństwa,
   c) przetwarzać dane w sposób inny niż opisany instrukcją technologiczną.

Załącznik Nr 4
do „Polityki bezpieczeństwa
i instrukcji zarządzania systemem informatycznym
w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju”

…….. Trzcińsko-Zdrój, dn. ……..
(imię i nazwisko pracownika)

……..
(adres)
……..

OŚWIADCZENIE

(tekst oświadczenia podpisanego przez pracowników Ośrodka Pomocy Społecznej oraz innych osób zatrudnionych w ramach przygotowania zawodowego lub praktyk)

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:
   a) o ochronie i postępowaniu z wiadomościami, stanowiącymi tajemnicę służbową,
   b) o zasadach ochrony oraz środkach i zabezpieczeniach danych osobowych (Dz. U. Nr 133 poz. 833) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 28 kwietnia 2004 roku (Dz. U. Nr 100 poz. 1024 z 2004 r.) oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych.
2 Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy w OPS, a w szczególności nie będę:
   a) ujawniać danych zawartych w eksploatowanych w OPS systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tym systemach,
   b) ujawniać szczegółów technologicznych używanych w OPS systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośniki magnetyczne i optyczne oraz wydruki komputerowe,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją technologiczną.

…….. ……
(podpis pracownika) (podpis przełożonego)

Załącznik Nr 7 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju”

Wzór

Raport

z naruszenia bezpieczeństwa systemu informatycznego w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju

1. Data: …… Godzina: ……
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……..
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

……..
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……..
……..
……..

5. Przyczyny wystąpienia zdarzenia:
……..
……..
……..

6. Podjęte działania:
……..
……..
……..

7. Postępowanie wyjaśniające:
……..
……..
……..

……..
(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 8 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju”

Wzór

Wykaz osób,
które zostały zapoznane z „Polityką bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
w Ośrodku Pomocy Społecznej w Trzcińsku-Zdroju,
przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis