Zarządzenie 15.2013
Dyrektora Powiatowego Centrum Pomocy Rodzinie
w Mińsku Mazowieckim
z dnia 18 grudnia 2013 roku

w sprawie: wprowadzenia Polityki Bezpieczeństwa Ochrony i Przetwarzania Danych Osobowych w Powiatowym Centrum Pomocy Rodzinie w Mińsku Mazowieckim

Na podstawie § 3 ust. 1 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 § 6 pkt 2 Regulaminu Organizacyjnego Powiatowego Centrum Pomocy Rodzinie w Mińsku Mazowieckim, stanowiącego załącznik do Uchwały Nr 240/12 Zarządu Powiatu Mińskiego z dnia 28 lutego 2012 roku

zarządzam co następuje:

§ 1

Wprowadzam Politykę Bezpieczeństwa Ochrony i Przetwarzania Danych Osobowych w Powiatowym Centrum Pomocy Rodzinie w Mińsku Mazowieckim, która stanowi załącznik do niniejszego zarządzenia.

§ 2

Traci moc Zarządzenie Nr 4/2010 Dyrektora Powiatowego Centrum Pomocy Rodzinie w Mińsku Mazowieckim z dnia 12 lutego 2010 roku w sprawie wprowadzenia w Powiatowym Centrum Pomocy Rodzinie w Mińsku Mazowieckim „Instrukcji w sprawie ochrony danych osobowych, zabezpieczania dokumentów zawierających dane osobowe oraz postępowania w przypadku stwierdzenia ich naruszenia” i Zarządzenie Nr 5/2010 Dyrektora Powiatowego Centrum Pomocy Rodzinie w Mińsku Mazowieckim z dnia 12 lutego 2010 roku w sprawie ochrony danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Mińsku Mazowieckim.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

POLITYKA BEZPIECZEŃSTWA OCHRONY I PRZETWARZANIA DANYCH OSOBOWYCH

W

POWIATOWYM CENTRUM POMOCY RODZINIE

W MIŃSKU MAZOWIECKIM

I. CEL POLITYKI

Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w Powiatowym Centrum Pomocy Rodzinie w Mińsku Mazowieckim przez pracowników i współpracowników, którzy przetwarzają dane osobowe.

Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez Powiatowe Centrum Pomocy Rodzinie w Mińsku Mazowieckim rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

II. ŹRÓDŁA WYMAGAŃ

Polityka bezpieczeństwa przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Mińsku Mazowieckim, zwana dalej Polityką została wydana w związku z § 3 ust. 1 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 zgodnie z:

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
- Wytycznymi w zakresie opracowania i wdrożenia polityki bezpieczeństwa - Generalny Inspektor Ochrony Danych Osobowych

III. ZAKRES STOSOWANIA

Politykę stosuje się do danych osobowych przetwarzanych w systemie informatycznym, danych osobowych zapisanych na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

W zakresie podmiotowym, Polityka obowiązuje wszystkich pracowników Powiatowego Centrum Pomocy Rodzinie w Mińsku Mazowieckim oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło.

IV. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

Przez bezpieczeństwo przetwarzania danych osobowych rozumie się zapewnienie:

- poufności — właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
- integralności — właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalności — właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

V. POZIOM BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Przy przetwarzaniu danych osobowych należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia, ponieważ urządzenia systemu służącego do przetwarzania danych osobowych połączone są z siecią publiczną.

VI. DEFINICJE

1. Administrator Danych Osobowych (ADO) – podmiot, który decyduje o środkach i celach przetwarzania danych osobowych. ADO w Powiatowym Centrum Pomocy Rodzinie jest Dyrektor..
2. Administrator Bezpieczeństwa Informacji (ABI) – osoba wyznaczona przez Dyrektora, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
3. Administrator Systemu Informatycznego (ASI)– osoba odpowiedzialna za funkcjonowanie systemu informatycznego w Centrum, informatyk zatrudniony w Centrum.
4. 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 lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
5. Centrum – Powiatowe Centrum Pomocy Rodzinie w Mińsku Mazowieckim.
6. Pracownik – osoba zatrudniona w formie umowy o pracę lub umowy cywilno-prawnej.
7. Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Administratora Danych Osobowych lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.
8. Przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
9. 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).
10. Ustawa – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
11. Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.
12. Zbiór nieinformatyczny - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem

informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

VII. ODPOWIEDZIALNOŚĆ

1. Dyrektor:

Do obowiązków Dyrektora należy zrozumienie oraz zapewnienie świadomości bezpieczeństwa przetwarzania danych osobowych, jego problematyki oraz wymagań. Do obowiązków należy również:

- podejmowanie odpowiednich i niezbędnych korków majach na celu zapewnienie prawidłowej ochrony danych osobowych;
- podział zdań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie Administratora Bezpieczeństwa Informacji.
- wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych;
- egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych;
- poddawanie przeglądom skuteczność polityki bezpieczeństwa przetwarzania danych osobowych;
- zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;
- zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
- zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych.

2. Administrator Bezpieczeństwa Informacji

Do obowiązków Administratora Bezpieczeństwa Informacji, należy nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej. Do obowiązków należy również:

- określenie wymagań bezpieczeństwa przetwarzania danych osobowych;
- nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych;
- prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury);
- analizę sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie oraz przedstawienie Zarządowi zaleceń i rekomendacji dotyczących eliminacji ryzyk ich ponownego wystąpienia.

3. Osoby upoważnione do przetwarzania danych, ewidencja według wzoru stanowiącego załącznik nr 2 do niniejszej Polityki

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej. Do obowiązków należy również:

- przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;
- postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;

- zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia;
- ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
- informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do przełożonego, który ma obowiązek poinformować Administratora Bezpieczeństwa Informacji.

VIII. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

1. Podstawowe zasady
   1) Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych.
   2) Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.
   3) Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
   4) Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

2. Procedury postępowania z danymi osobowymi
   1) Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
   2) Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
   3) Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

3. Upoważnienie do przetwarzania danych osobowych
   1) Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 37 Ustawy.
   2) Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Bezpieczeństwa Informacji.
   3) W celu upoważnienia do przetwarzania danych osobowych należy dostarczyć do Administratora Bezpieczeństwa Informacji podpisane oświadczenie, którego wzór stanowi załącznik nr 6 niniejszej Polityki.
   4) Na podstawie otrzymanego oświadczenia Administrator Bezpieczeństwa Informacji upoważnia formalnie wnioskującego do przetwarzania danych osobowych i wydaje upoważnienie sporządzane wg wzoru stanowiącego załącznik nr 7 niniejszej Polityki.
   5) Upoważnienia, o których mowa powyżej przechowywane są i obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.

4. Ewidencja osób upoważnionych
   1) Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji i zawiera w szczególności:
      - imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych;

- zakres upoważnienia do przetwarzania danych osobowych;
- identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych;
- datę nadania i odebrania uprawnień.

5. Zachowanie danych osobowych w tajemnicy

Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

6. Znajomości regulacji wewnętrznych

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w Centrum, w szczególności Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

7. Zgodność

1) Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Centrum, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2) Okresowy przegląd Polityki powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Centrum oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.
3) Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w Centrum.

IX. ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI

1. Bezpieczeństwo usług zewnętrznych

1) Należy zapewnić aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w Centrum, wymaganiami umowy oraz wymaganiami prawa.
2) Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić w umowie świadczenia usług.
3) Należy zapewnić aby użytkownicy nie będący pracownikami Centrum stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.

2. Powierzanie przetwarzania danych osobowych

Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy.

1) Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 31 i nast. Ustawy. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem

przetwarzania danych do podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36-39a Ustawy.

2) W umowach stanowiących podstawę powierzenia przetwarzania danych albo eksploatacji systemu informatycznego lub części infrastruktury należy umieścić zobowiązanie podmiotu zewnętrznego do przestrzegania niniejszej Polityki oraz zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych.
3) Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Centrum za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa Centrum do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa.

3. Udostępnianie danych osobowych

1) Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
2) Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora Bezpieczeństwa Informacji.
3) Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
4) Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o udostępnieniu bezpośrednio w systemie informatycznym z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych.
5) Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

4. Monitorowanie i przegląd usług strony trzeciej

Monitorowanie usług strony trzeciej powinno być udokumentowane i powinno zawierać informacje o: poziomie wykonania usługi, incydentach bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych, śladach audytowych, problemach operacyjnych, awariach, błędach i zakłóceniach.

X. BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA

1. Obszar przetwarzania

1) Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Centrum prowadzi działalność. Do takich pomieszczeń, zalicza się w szczególności:
   - pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
   - pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe;
   - pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.

2) Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.
3) Osoby upoważnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku drzwi. Nie można wynosić ww. kluczy po zakończeniu pracy poza miejsca przeznaczone do ich przechowywania.
4) Wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
5) Niepotrzebne wydruki lub inne dokumenty należy niszczyć za pomocą niszczarek.
6) Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.
7) Szczegółowy wykaz obszarów przetwarzania danych osobowych znajduje się w załączniku nr 3 niniejszej Polityki.

2. Bezpieczeństwo środowiskowe
1) Lokalizację i umiejscowienie danych osobowych należy starannie dobierać z uwzględnieniem wymaganych aspektów bezpieczeństwa przetwarzania danych osobowych. W szczególności należy rozważyć aspekty dotyczące:
   - zasilania energią elektryczną;
   - klimatyzacji oraz wentylacji;
   - wykrywania oraz ochrony przed pożarem i powodzią;
   - fizycznej kontroli dostępu.
2) Pomieszczenia wchodzące w skład obszaru przetwarzania danych osobowych należy wyposażyć w odpowiednie środki ochrony fizycznej i organizacyjnej chroniące przed nieautoryzowanym lub nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami pracy.
3) Kopie zapasowe zawierające dane osobowe należy przechowywać w metalowej szafie.

3. Bezpieczeństwo urządzeń
1) Urządzenia służące do przetwarzania danych osobowych należy przechowywać w bezpieczny i nadzorowany sposób.
2) Urządzenia mobilne takie jak np. komputery przenośne, urządzenia PDA, telefony komórkowe nie powinny być pozostawiane bez opieki jeżeli nie są zastosowane odpowiednie środki ochrony.

4. Fizyczna kontrola dostępu
1) Należy wdrożyć procedury eksploatacyjne w celu ochrony danych osobowych oraz dokumentacji systemowej przed nieautoryzowanym lub nieuprawnionym ujawnieniem, modyfikacją, usunięciem i zniszczeniem.
2) Należy wdrożyć politykę czystego biurka i czystego ekranu w celu redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia danych osobowych.
3) Klucze dostępowe, karty, hasła itd. służące do uzyskania dostępu do systemów informatycznych służących do przetwarzania danych osobowych należy zabezpieczać a sposób ich uzyskiwania należy szczegółowo zdefiniować w procedurach.

4) Dostęp do serwerowni lub innych pomieszczeń, w których znajdują się systemy informatyczne służące do przetwarzania danych osobowych lub zbiory nieinformatyczne należy rejestrować oraz okresowo przeglądać.
5) Dostęp dla gości do serwerowni lub innych pomieszczeń, w których znajdują się systemy informatyczne służące do przetwarzania danych osobowych należy nadzorować przez cały czas ich pobytu.
6) Przyznawanie dostępu gościom należy wykonywać wyłącznie w określonych i autoryzowanych celach.
7) Kończąc pracę, należy zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację, wydruki, elektroniczne nośniki informacji i umieścić je w zamykanych szafkach.
8) Monitory należy ustawić w taki sposób aby uniemożliwiać podgląd wyświetlanych danych osobowych przez osoby nieuprawnione.
9) W przypadku korzystania z usług zewnętrznych podmiotów oferujących zbieranie i niszczenie papierów, urządzeń lub nośników zwierających dane osobowe, należy wybrać wykonawcę z odpowiednimi zabezpieczeniami i doświadczeniem.

XI. ZARZĄDZANIE INCYDENTAMI

1. Monitorowanie incydentów
   1) Incydenty związane z bezpieczeństwem przetwarzania danych osobowych powinny być wykrywane, rejestrowane i monitorowane w celu ich zidentyfikowania i zapobiegania ich wystąpieniu w przyszłości.
   2) Zdarzenia systemowe powinny być przechowywane jako materiał dowodowy zaistniałych incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.
   3) Użytkownicy systemów powinni znać i przestrzegać zasad zgłaszania incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.

2. Zgłaszanie incydentów

Zaistniałe zdarzenia związane z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa przetwarzania danych osobowych takie jak np. utrata integralności, niedostępność, awarie, uszkodzenia, ostrzeżenia i alarmy bezpieczeństwa systemów informatycznych, urządzeń teleinformatycznych oraz danych powinny być niezwłocznie zgłaszane do Administratora Bezpieczeństwa Informacji.

XII. ZBIORY DANYCH OSOBOWYCH

1. Wykaz zbiorów danych osobowych
   1) Dokumentacja zbiorów danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji i stanowi załącznik nr 1 niniejszej Polityki.
   2) Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń należących do obszaru przetwarzania danych osobowych.
2. Opis struktury zbiorów danych osobowych
   1) Dokumentacja zbiorów danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji i stanowi załącznik nr 4 niniejszej Polityki.

2) Wskazane w załączniku nr 4 zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych oraz powiązania pól informacyjnych utworzonych w tych systemach.
3) Zawartość pól informacyjnych, występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają Administratora Danych Osobowych do przetwarzania danych osobowych.

3. Sposób przepływu danych pomiędzy poszczególnymi systemami
1) Dokumentacja systemów informatycznych służących do przetwarzania danych osobowych powinna zawierać opis współpracy z innymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami z którymi współpracuje, stanowi to załącznik nr 5 niniejszej Polityki.
2) Administrator systemów informatycznych jest zobowiązany do poprowadzenia aktualnej dokumentacji opisującej sposób przepływu danych osobowych pomiędzy systemami.

XIII. METODY I ŚRODKI UWIERZYTELNIANIA ORAZ OPIS PROCEDUR ZWIĄZANYCH Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

Każdy użytkownik posiada swoje hasło. Hasła przekazywane są w formie ustnej. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się co najmniej z 6 lub 8 znaków – w zależności od tego, czy w systemie są przetwarzane dane wrażliwe. Osobą odpowiedzialną za przydział haseł jest Administrator Bezpieczeństwa Informacji. Użytkownik po otrzymaniu hasła jest zobowiązany do niezwłocznej jego zmiany, chyba że system nie umożliwia wykonania takiej operacji. Użytkownik sam musi pamiętać o konieczności i terminie zmiany hasła. Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej. Pracownicy o każdorazowym awaryjnym użyciu hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych informują Administrator Bezpieczeństwa Informacji.

XIV. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowana z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogować się z sieci komputerowej
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

XV. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Za systematyczne przygotowanie kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania odpowiada osoba mająca upoważnienie do ich przetwarzania.
2. Kopie zapasowe zbiorów danych oraz programów i narzędzi służących do ich przetwarzania wykonywane są codzienne po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
3. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym dniu każdego miesiąca w postaci zapisu na płytach CD-R lub DVD-R.
4. Płyty CD-R/DVD-R przechowuje się w skarbczyku w metalowej szafie.

XVI. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM (§ 5 PKT 2 ROZPORZĄDZENIA)

1. Za ochronę antywirusową odpowiada ASI;
2. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI, wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego;
3. Oprogramowanie antywirusowe pracuje na serwerach oraz w miarę możliwości, na wszystkich stanowiskach sieciowych;
4. Aktualizacja oprogramowania antywirusowego winna odbywać się nie rzadziej niż raz w tygodniu, w sposób automatyczny dla całej sieci lokalnej;
5. Użytkownik systemu na stanowisku komputerowym, importujący dane osobowe do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów;

XVII. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ PROGRAMÓW I NARZĘDZI SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Przeglądy i konserwacja urządzeń:
   1) przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu;
   2) nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

2. Przegląd programów i narzędzi programowych:
   1) konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów;
   2) Administrator Bezpieczeństwa Informacji zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję;

3. Należy prowadzić Rejestrację działań konserwacyjnych, awarii oraz napraw.

XVIII. DOKUMENTY POWIĄZANE

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Centrum, załącznik nr 8 do niniejszej Polityki.
2. Instrukcja postępowania w sytuacji naruszenia danych osobowych w Centrum, załącznik nr 9 do niniejszej Polityki.

XIX. POSTANOWIENIA KOŃCOWE

1) Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2) W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.
3) Pracownicy Centrum zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Centrum, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

DYREKTOR

Powiatowego Centrum Pomocy Rodzinie

Janusz Zdzieborski