Załącznik nr 1

do Zarządzenie nr 8/2012
Dyrektora Miejskiego Ośrodka Pomocy Społecznej
w Ostródzie z dnia 31 grudnia 2012 r.

Polityka bezpieczeństwa danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Ostródzie

I. Podstawa prawna

§ 1

Podstawą prawną do sporządzenia Polityki Bezpieczeństwa Danych osobowych, zwanej dale Polityką Bezpieczeństwa, jest art.36 oraz 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. Nr 101, poz. 926 z późn. zm., zwana dalej Ustawą 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), zwane dalej Rozporządzeniem.

II. Postanowienia ogólne

§ 2

1. Polityka bezpieczeństwa danych osobowych określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Ostródzie.
2. Celem wprowadzenia i wdrażania polityki bezpieczeństwa jest:
   - zapewnienie prawidłowości przetwarzania danych osobowych pod kątem legalności ich przetwarzania oraz ochrony w czasie całego procesu przetwarzania, tj. wykonywania jakiekolwiek operacje na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemach informatycznych,
   - maksymalne ograniczenie ryzyka związanego z nieuprawnionym przetwarzaniem lub utratą danych osobowych,
   - podejmowanie wszelkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów osób, których dane są przetwarzane,
   - podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane osobowe w zakresie problematyki bezpieczeństwa tych danych.

§ 3

Polityka bezpieczeństwa obowiązuje wszystkich pracowników Miejskiego Ośrodka Pomocy Społecznej w Ostródzie, a także osoby wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoby odbywające staż, praktyki lub będące wolontariuszami oraz inne osoby - jeżeli działania tych osób wiążą się z przetwarzaniem przez te osoby danych osobowych.

III. Osoby odpowiedzialne za nadzór nad przetwarzanie danych osobowych

§ 4

1. Nadzór ogólny nad realizacją przepisów wynikających z Ustawy oraz Rozporządzenia pełni Administrator Danych.
2. Administratorem Danych Osobowych (ADO) przetwarzanych w Miejskim Ośrodku Pomocy Społecznej w Ostródzie jest Dyrektor Ośrodka.
3. Do zadań administrator danych osobowych należy w szczególności:
   - wyznaczenie administratora bezpieczeństwa danych osobowych,
   - dokonywanie zgłoszeń zbiorów danych osobowych Generalnemu Inspektorowi Ochrony Danych Osobowych,
   - zatwierdzanie procedur dot. przetwarzania danych osobowych,
   - udzielanie i cofanie upoważnień do przetwarzania danych osobowych.

§ 5

1. Administrator Danych Osobowych wyznacza pracownika Ośrodka lub inna osobę do pełnienia roli Administratora Bezpieczeństwa Informacji (ABI), do którego obowiązków należy nadzorowanie przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych oraz prowadzenie i aktualizacja rejestrów i wykazów przewidzianych niniejszym dokumentem.
2. Administrator Bezpieczeństwa Informacji pełni jednocześnie rolę Administratora Bezpieczeństwa Informacji PEFS 2007
3. Administrator Danych wyznacza także osobę do pełnienia roli Administratora Bezpieczeństwa Informacji dla Miejskiego Zespołu Interdyscyplinarnego.

§ 6

1. Osobą odpowiedzialną za nadzór i koordynującą prace w zakresie eksploatacji, monitorowania i praw dostępu do zasobów informatycznych gromadzonych i przetwarzanych w sieci informatycznej jest Administrator Systemów Informatycznych (ASI), którego rolę pełni osoba zatrudniona na stanowisku informatyka.
2. W okresie nieobecności w pracy Administratora Systemów Informatycznych zastępuje go Administrator Bezpieczeństwa Informacji.

IV. Obszar, w którym przetwarzane są dane osobowe

§ 7

1. Dane osobowe przetwarzane są zarówno w formie tradycyjnej (papierowej), jak też w formie elektronicznej z wykorzystaniem systemów informatycznych w następujących budynkach przekazanych w trwały zarząd Miejskiemu Ośrodkowi Pomocy Społecznej w Ostródzie:
   - siedziba Ośrodka Ostróda ul.Olsztyńska 2,
   - budynek położony w Ostródzie ul.11-go Listopada 25.
2. Wykaz pomieszczeń, w których przetwarzane są dane osobowe zawiera załącznik nr 1 do Polityki Bezpieczeństwa.

V. Zbiory danych osobowych

§ 8

1. Przetwarzanie danych osobowych dopuszczalne jest wyłącznie na zasadach określonych w Ustawie i jedynie w celu, w jakim dane te zostały zebrane, gdy:
   1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,

2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

2. Przetwarzania danych 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 jest dopuszczalne jedynie w sytuacji, gdy:
1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,
2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
4) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
5) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
6) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą
7) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

§ 9

1. Administrator Danych zobowiązany jest do informowania osób, których dane są zbierane, o adresie swojej siedziby i pełnej nazwie, celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, prawie dostępu do treści danych treści oraz do ich poprawiania, dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej, a także o źródle danych, jeżeli są one zbierane nie od osoby, której dotyczą.
2. Powyższy obowiązek nie istnieje, jeżeli:
1) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 2,
2) w przypadku zbierania danych od osoby, której dotyczą - przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
3) w przypadku zbierania danych osobowych nie od osoby, której one dotyczą:
- przepis ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
- dane są przetwarzane na podstawie przepisów prawa.
3. Osobie, której dane są przetwarzane, przysługuje prawo do kontroli tego przetwarzania w zakresie określony przepisami Ustawy.

§ 10

1. Udostępnianie danych osobowych dopuszczalne jest wyłącznie w trybie przewidzianym w Ustawie.

2. Decyzję o udostępnieniu danych osobowych podejmuje Administrator Danych Osobowych, bądź kierownicy poszczególnych działów z upoważnienia i w zakresie przez niego określonym.
3. W przypadku udostępnienia danych osobowych przetwarzanych w systemach informatycznych - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - winny zostać odnotowane w tych systemach informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.
4. Za odnotowanie w systemie informatycznym informacji, których mowa w ust.3 odpowiedzialna jest osoba, która dane te udostępnia.
5. Dopuszcza się możliwość powierzenia przetwarzania danych osobowych na zasadach określonych w art.31 Ustawy.

§ 11

1. Wykaz zbiorów danych osobowych, które przetwarzane są w Miejskim Ośrodku Pomocy Społecznej zawiera załącznik nr 2 do Polityki Bezpieczeństwa.
2. Wykaz zbiorów danych ze wskazaniem programów zastosowanych do przetwarzania tych danych zawiera załącznik nr 3 do Polityki Bezpieczeństwa

VI. Osoby przetwarzające dane osobowe

§ 12

1. Każda osoba przed podjęciem zatrudnienia, rozpoczęciem stażu, praktyk w Miejskim Ośrodku Pomocy Społecznej w Ostródzie winna zostać zapoznana z przepisami dotyczącymi ochrony danych osobowych oraz odpowiednimi dokumentami obowiązującymi w tym zakresie w Ośrodku, potwierdzając ten fakt przez złożenie oświadczenia (załącznik nr 4 do Polityki Bezpieczeństwa).
2. W przypadku osób realizujących na rzecz Miejskiego Ośrodka Pomocy Społecznej w Ostródzie Ośrodka umowy cywilno-prawne, działających jako wolontariusze, a także wykonującego inne czynności, powyższy obowiązek występuje jedynie w przypadku, gdy wykonywane działania wiążą się z dostępem lub przetwarzaniem danych osobowych znajdujących się w zbiorach danych Ośrodka.

§ 13

1. Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora danych Osobowych.
2. Wzór upoważnienia do przetwarzania danych osobowych zawiera załącznik nr 5 do Polityki Bezpieczeństwa, w przypadku projektów realizowanych w ramach Programu Operacyjnego Kapitał Ludzki wzór upoważnienia do przetwarzania danych osobowych uczestników projektu określają załączniki do umowy o finansowanie projektu.
3. Administrator Bezpieczeństwa Informacji prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych oraz rejestr osób upoważnionych do przetwarzania danych osobowych uczestników projektu realizowanego w ramach Programu Operacyjnego Kapitał Ludzki.
4. Administrator Bezpieczeństwa Informacji prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych, a także rejestr osób upoważnionych do przetwarzania danych osobowych w Formularzu PEFS 2007 - załącznik nr 6 do Polityki Bezpieczeństwa.

VII. Struktury zbiorów danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami

§ 14

1. Opis struktury zbiorów wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi zawarty jest w załączniku nr 7 do Polityki Bezpieczeństwa.
2. Sposób przepływu danych pomiędzy poszczególnymi systemami przedstawiony jest w załączniku nr 8 do Polityki Bezpieczeństwa

VIII. Środki techniczne i organizacyjne służące ochronie obszaru, w którym przetwarzane są dane osobowe

§ 15

1. Budynki Ośrodka poza godzinami jego funkcjonowania chronione są systemem alarmowym, monitorowanym przez firmę zewnętrzną.
2. Administrator Bezpieczeństwa Informacji prowadzi rejestr osób posiadających dostęp do kluczy od budynków oraz kodów do systemu alarmowego.
3. Klucze do pomieszczeń wydawane są bezpośrednio osobom pracującym w danym pomieszczeniu i od nich są po zakończeniu pracy odbierane.
4. Pomieszczenia, w których przetwarzane są dane osobowe w czasie nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, muszą być zamykane w sposób uniemożliwiający dostęp do nich osobom postronnym
5. Pomieszczenia, w których przetwarzane są dane osobowe sprawdzane są okresowo pod względem zabezpieczeń (zamki, alarm) uniemożliwiających dostęp do nich osób postronnych.

§ 16

1. Wewnątrz obszaru, w którym przetwarzane są dane osobowe przebywanie osoby nieuprawnionej dopuszczalne jest za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
2. Dane osobowe, zarówno w formie papierowej, jak też z użyciem systemu informatycznego przetwarzane są w godzinach pracy Ośrodka w wyznaczonym do tego obszarze. Przetwarzanie danych osobowych w innym terminie dopuszczalne jest jedynie w uzasadnionych przypadkach, za wiedzą i zgodą Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji.
3. Przetwarzanie danych osobowych poza wyznaczonym obszarem dopuszczalne jest w przypadku pracowników socjalnych, do których obowiązków należy przeprowadzanie rodzinnych wywiadów środowiskowych, a także w przypadku innych pracowników, w zakresie, w jakim realizacja ich obowiązków wymaga pozyskiwania danych poza budynkami ośrodka.

IX. Środki techniczne i organizacyjne służące ochronie danych przetwarzanych w formie papierowej

§ 17

1. Pracownicy, którzy przetwarzają dane osobowe w formie papierowej, zobowiązani są do zabezpieczenia tych danych przed dostępem osób niemających upoważnienia do przetwarzania tych danych.
2. Zbiór danych osobowych w formie papierowej winien być przechowywany w meblowych szafach zamykanych na zamki.
3. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp do nich osobom nieupoważnionym.
4. Dokumenty zawierające dane osobowe po ustaniu ich przydatności winny być archiwizowane stosowne do obowiązujących w Miejskim Ośrodku Pomocy Społecznej

w Ostródzie przepisów, bądź niszczone w sposób mechaniczny za pomocą niszczarek do papieru .

5. Do momentu zarchiwizowania lub zniszczenia dokumenty należy przechowywać w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym miejscu, do którego osoby postronne nie mają dostępu.

X. Środki techniczne i organizacyjne służące ochronie danych przetwarzanych w systemach informatycznych

§ 18

1. Pomieszczenie, w którym znajdują się serwery i bazy danych chronione jest poza godzinami pracy ośrodka system alarmowym, jest klimatyzowane, posiada okratowane okna i drzwi antywłamaniowe
2. Dostęp do pomieszczenia, o którym mowa w ust.1 podlega kontroli, Administrator Bezpieczeństwa Informacji prowadzi rejestr osób posiadających dostęp do tego pomieszczenia
3. Sprzęt komputerowy zasilany jest odrębną sieć elektryczną.
4. Przed awariami zasilania i zakłóceniami w sieci energetycznej serwery, na których znajdują się bazy danych zabezpieczone są zasilaczami awaryjnymi.
5. Administrator Systemów Informatycznych nie rzadziej niż raz w miesiącu sprawdza poprawność działania zasilaczy awaryjnych.

§ 19

1. W celu ochrony zbioru danych osobowych przed utratą lub celowym zniszczeniem, wszystkie bazy zawierające dane osobowe są kopiowane zgodnie z procedurami opisanymi w Instrukcji Zarządzania Systemem Informatycznym.
2. 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.
3. W przypadku naprawy sprzętu komputerowego zawierającego dane osobowe dane te są wcześniej usuwane, a w przypadku braku takiej możliwości naprawa odbywa się pod nadzorem Administrator Systemów Informatycznych.
4. Nośniki służące przenoszeniu danych pomiędzy systemami informatycznymi, winny być po dokonaniu przeniesienia danych pozbawiane zapisu.

§ 20

1. Przetwarzanie danych osobowych w bazach danych odbywa się w oparciu o architekturę klient-serwer, stanowiska komputerowe, do których dostęp posiadają pracownicy, są jedynie końcówkami klienckimi, a przetwarzanie danych przy pomocy uruchamianych na poszczególnych stanowiskach aplikacji odbywa się bezpośrednio na serwerach.
2. Dostęp zarówno do samego systemu informatycznego, jak też do aplikacji służących do przetwarzania danych osobowych, wymaga dokonania przez użytkownika autoryzacji poprzez wpisanie indywidualnego identyfikatora i hasła.
3. Użytkownik, od momentu otrzymania indentyfikatora, ponosi odpowiedzialność za czynności, które zostały wykonane przy jego użyciu.

§ 21

1. Ochrona antywirusowa serwerów i stacji roboczych podłączonych do sieci odbywa się w czasie rzeczywistym, a aktualizacje oprogramowania antywirusowego pobierane są automatycznie.
2. Automatycznie dokonuje się także aktualizacja system operacyjnego na stacjach roboczych.

3. W przypadku korzystania ze stacji roboczych niepodłączonych do sieci, aktualizacje oprogramowania antywirusowego oraz systemu operacyjnego wykonuje Administrator Systemów Informatycznych.
4. Administrator Systemów Informatycznych na bieżąco wykonuje aktualizacje aplikacji specjalistycznych.

§ 22

1. Monitory komputerów, na których są przetwarzane dane osobowe, winny być ustawione w sposób uniemożliwiający wgląd osobom nieupoważnionym w przetwarzane dane.
2. W przypadku braku takiej możliwości, należy zastosować osłonę w formie odpowiedniego filtru na ekran lub stworzyć możliwość natychmiastowego użycia wygaszacza ekranu.
3. Na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe, winny być zainstalowane automatyczne wygaszacze ekranu blokujące po 10 minutach bezczynności dostęp do stacji roboczej i wymagające ponownego zalogowania się przez użytkownika do systemu.
4. Każdy użytkownik przed czasowym opuszczeniem stanowiska pracy zobowiązany jest do blokowania stacji roboczej przed osobami postronnymi poprzez wylogowanie się z systemu, bądź zastosowanie wygaszacza ekranu.
5. Całkowicie zakazane jest udostępnianie komputera zawierającego dane osobowe osobom nieupoważnionym.

XI. Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 23

Na pracownikach Miejskiego Ośrodka Pomocy Społecznej w Ostródzie oraz innych osobach przetwarzających dane osobowe w Ośrodku ciąży obowiązek niezwłocznego zawiadomienia Administratora Bezpieczeństwa Informacji w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, zarówno przetwarzanych w formie papierowej, jak też w systemach Informatycznych, a w szczególności o :

1) kradzieży, zaginięciu, uszkodzeniu danych osobowych przetwarzanych w formie papierowej, wejścia w ich posiadanie lub przetwarzanie ich przez osoby nieupoważnione,
2) naruszeniu zabezpieczeń systemu informatycznego, ujawnieniu haseł, braku możliwości zalogowania się do systemu lub aplikacji, w której przetwarzane są dane osobowe, bądź braku możliwości przetwarzania w tych aplikacjach,
3) pojawieniu się komunikatu alarmowego wskazującego na nieprawidłowe funkcjonowanie systemów informatycznych,
4) pogorszeniu się jakości transmisji danych w sieciach komputerowych mogącej wskazywać na naruszenie zabezpieczeń tych danych,
5) pogorszeniu się technicznego stanu urządzeń,
6) stwierdzeniu nieuprawnionych zmian zawartości zbioru danych osobowych,
7) niezachowaniu podstawowym zasad dotyczących zabezpieczenia danych osobowych (niezablokowanie dostępu do aplikacji przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, bądź w ksero, niezamknięcie pomieszczenia, w którym przetwarzane są dane osobowe w czasie nieobecności w nim, przechowywanie danych osobowych w sposób pozwalający na dostęp do nich osobom nieupoważnionym, etc.)
8) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (pożar, brak energii elektrycznej, zalanie pomieszczeń, itp).

§ 24

1. Administrator Bezpieczeństwa Informacji zobowiązany jest niezwłocznie podjąć działania w celu wyeliminowania zgłoszonych naruszeń lub zagrożeń naruszenia

ochrony danych osobowych i przywrócenia stanu umożliwiającego prawidłowe przetwarzanie danych osobowych

2. Administrator Bezpieczeństwa Informacji prowadzi rejestr zgłoszonych zdarzeń dotyczących naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, w którym winien w szczególności:
   1) wskazać osobę, która dokonała zawiadomienia oraz kiedy to nastąpiło,
   2) podać czas i miejsce naruszenia ochrony danych osobowych,
   3) określić, jakiego rodzaju naruszenie nastąpiło i w jakich okolicznościach,
   4) ustalić, jaki był wpływ naruszenia na przetwarzane dane osobowe,
   5) opisać podjęte działania oraz przedstawić ocenę przyczyn wystąpienia naruszenia,
   6) przedstawić propozycję postępowania mającego na celu zapobiegniecie podobnym zdarzeniom w przyszłości.
3. W przypadku, gdy zgłoszenie dotyczy naruszeń ochrony systemów informatycznych, rejestr, o którym mowa w ust.1 prowadzony jest przez Administratora Systemów Informatycznych.

§ 25

1. Naruszenie obowiązków dotyczących ochrony danych osobowych przez osobę zatrudnioną przy przetwarzaniu danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych i podlegać sankcjom przewidzianym w Regulaminie Pracy.
2. Osoba naruszająca przepisy ustawy o ochronie danych osobowych może także podlegać odpowiedzialności karnej przewidzianej w tej ustawie.