Załącznik Nr 1
do Zarządzenia Nr 91/2012
Dyrektora Miejskiego Ośrodka
Pomocy Społecznej w Bydgoszczy
z dnia 5 grudnia 2012r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

w
Miejskim Ośrodku Pomocy Społecznej
w Bydgoszczy

Spis Treści

Podstawa prawna.....
Podstawowe pojęcia.....

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I.1 Wykaz budynków, w których przetwarzane są dane osobowe.....
I.2 Zbiory danych przetwarzanych w systemach informatycznych i opis struktury przetwarzanych danych osobowych.....
I.3 Zbiory danych przetwarzanych tradycyjnie.....
I.4 Środki techniczne i organizacyjne stosowane w przetwarzaniu danych.....
I.4.1 Cele i zasady funkcjonowania polityki bezpieczeństwa.....
I.4.2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych.....
I.4.3 Zasady udzielania dostępu do danych osobowych.....
I.4.4 Udostępnianie i powierzanie danych osobowych.....
I.4.5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej..
I.4.6 Bezpieczeństwo w przetwarzaniu danych osobowych w systemach Informatycznych.....
I.5 Analiza ryzyka związanego z przetwarzaniem danych osobowych.....
I.5.1 Identyfikacja zagrożeń.....
I.5.2 Sposób zabezpieczenia danych.....
I.5.3 Określenie wielkości ryzyka.....
I.5.4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń.....

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

II.1 Procedury nadawania i zmiany uprawnień do przetwarzania danych w systemie informatycznym.....
II.2 Zabezpieczanie danych w systemie informatycznym.....
II.3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym.....
II.4 Tworzenie kopii zapasowych.....
II.5 Udostępnianie danych.....
II.6 Przeglądy i konserwacje systemów.....
II.7 Niszczenie wydruków i nośników danych.....

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

III.1 Istota naruszenia danych osobowych.....
III.2 Postępowanie w przypadku naruszenia danych osobowych.....
III.3 Sankcje karne.....

ZAŁĄCZNIKI

Podstawa prawna:

1. Konstytucja RP (art. 47 i 51),
2. Konwencja Nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych,
3. Dyrektywa PE i RE z dnia 24 października 1995r. (95/46/EC), w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych,
4. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r. Nr 101, poz. 926, z późn. zm.),
5. Rozporządzenie MSWiA z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004r. Nr 100, poz. 1024);
6. Ustawa z dnia 26 czerwca 1974r. - Kodeks pracy (Dz.U. z 1998r. Nr 21, poz. 94, z późn. zm.),
7. Ustawa z dnia 12 marca 2004r. o pomocy społecznej (Dz.U. z 2009r. Nr 175, poz. 1362 z późn. zm.),
8. Ustawa z dnia 7 września 2007r. o pomocy osobom uprawnionym do alimentów (Dz.U. z 2007r. Nr 192, poz. 1378)

Podstawowe pojęcia:

1. Ośrodek – w tym dokumencie jest rozumiany, jako Miejski Ośrodek Pomocy Społecznej w Bydgoszczy przy ul. Ogrodowej 9, wraz ze wszystkimi komórkami organizacyjnymi i jednostkami działającymi przy Ośrodku, zgodnie ze schematem organizacyjnym, będącym załącznikiem Nr 1 do Zarządzenia Nr 79/11 Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Bydgoszczy z dnia 30 grudnia 2011r. w sprawie nadania regulaminu organizacyjnego Miejskiego Ośrodka Pomocy Społecznej w Bydgoszczy;
2. Polityka – w tym dokumencie rozumiana jako „Polityka bezpieczeństwa", obowiązująca w Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy;
3. Instrukcja – w tym dokumencie rozumiana jako „Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy;
4. Administrator Bezpieczeństwa Informacji (ABI) – pracownik Ośrodka wyznaczony przez Administratora Danych Osobowych (Dyrektora), do nadzorowania przestrzegania zasad ochrony danych osobowych oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy. ABI powołany jest zarządzeniem Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Bydgoszczy;
5. Użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w Ośrodku, osoba wykonująca pracę na podstawie umowy – zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Ośrodku;
6. Identyfikator użytkownika – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
7. Administrator Systemu Informatycznego (ASI) – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie;
8. Sieć lokalna – połączenie komputerów pracujących w Ośrodku, w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych;
9. Sieć publiczna – sieć telekomunikacyjna, nie będąca siecią wewnętrzną, służącą do świadczenia usług telekomunikacyjnych, w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz.U. Nr 73, poz. 852, z późn. zm.);
10. Sieć telekomunikacyjna – urządzenia telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną, w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz.U. Nr 73, poz. 852, z późn. zm.);
11. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych;
12. Przetwarzanie danych – są to jakiekolwiek operacje, wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
13. Zabezpieczenie danych w systemie informatycznym – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
14. Teletransmisja – przesyłanie informacji za pomocą sieci telekomunikacyjnej;
15. Aplikacja – program komputerowy, wykonujący konkretne zadanie;

16. Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną;
17. Dane osobowe – danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności, np. sama nazwa ulicy i numer domu, w którym mieszka wiele osób. Informacja ta będzie jednak stanowić dane osobowe wówczas, gdy zostanie zestawiona z innymi, dodatkowymi informacjami, np. imieniem i nazwiskiem czy numerem PESEL, które w konsekwencji można odnieść do konkretnej osoby;
18. Tożsamość – oznacza cechy, które stanowią o tym, kim dana osoba jest, czym różni się od innych. Na tak rozumianą tożsamość składa się nie tylko to, kim się jest obecnie, ale także to kim się było, a nawet zamierzenia na przyszłość, wszystko to powoduje, że dana osoba różni się od innej (vide: wyrok WSA z 3 marca 2009r., sygn. akt II S.A./Wa 1495/08);

Przykłady informacji stanowiącej dane osobowe:

Numer PESEL
Zgodnie z art. 31a ust. 1 ustawy o ewidencji ludności i dowodach osobistych, jest 11-cyfrowym, stałym symbolem numerycznym, jednoznacznie identyfikującym osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne cztery – liczbę porządkowa i płeć osoby, a ostatnia jest cyfrą kontrolną, służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego.

Numer ten, występując nawet bez zestawienia z innymi informacjami o osobie, stanowi dane osobowe.

Adres poczty elektronicznej
Adres poczty elektronicznej – bez dodatkowych informacji, umożliwiających ustalenie tożsamości osoby – zasadniczo nie stanowi danych osobowych. Występujący samodzielnie adres poczty można w wyjątkowych przypadkach uznać za dane osobowe, ale tylko wtedy, gdy elementy jego treści pozwalają, bez nadmiernych kosztów, czasu lub działań – na ustalenie na ich podstawie tożsamości danej osoby.

19. Dane szczególnie chronione
Dane szczególnie chronione wyliczone są w art. 27 ust. 1 ustawy. Są to informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, religijnych, filozoficznych, wyznaniu, przynależności do partii lub związku, stanie zdrowia, kodzie genetycznym, nałogach, postępowaniu przed sadem lub urzędem. Na administratorów tych danych ustawa nakłada bardziej rygorystyczne obowiązki, niż na administratorów danych „zwykłych".

20. Dane „zwykłe"
Nie jest to pojecie zdefiniowane w ustawie o ochronie danych osobowych. Pojęcie to obejmuje dane osobowe, których nie zalicza się do danych wrażliwych. Są to więc wszystkie dane osobowe poza wymienionymi w art. 27 ust. 1 ustawy. Zalicza się do nich np. imię, nazwisko, adres zamieszkania, datę urodzenia, nr PESEL, adres email.

21. Zgoda na przetwarzanie danych osobowych
Przez pojecie zgody osoby, której dane dotyczą – rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Wyrażenie zgody na przetwarzanie danych osobowych jest zbędne, gdy przetwarzanie danych jest dopuszczalne na podstawie: odrębnych przepisów prawa (np. w celu przeprowadzenia wywiadu środowiskowego przez pracownika pomocy społecznej) lub innych przesłanek (np. w celu realizacji umowy).

22. Usuwanie danych osobowych

Usuwanie danych osobowych to inaczej zniszczenie danych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Usuwanie danych oznacza więc takie procedury, których zastosowanie pozbawi administratora danych możliwości jakiegokolwiek dalszego przetwarzania danych osobowych.

I.1 Wykaz budynków, w których przetwarzane są dane osobowe

L.p.	Jednostka organizacyjna - adres	Pomieszczenia
1.	Miejski Ośrodek Pomocy Społecznej – Bydgoszcz ul. Ogrodowa 9	- wszystkie pomieszczenia biurowe
2.	Dział Realizacji Świadczeń i Pomocy Instytucjonalnej MOPS – Bydgoszcz ul. Toruńska 272	- wszystkie pomieszczenia biurowe
3.	Dział Rodzinnej Pieczy Zastępczej MOPS – Bydgoszcz ul. Toruńska 272	- wszystkie pomieszczenia
4.	Dział Wsparcia Rodziny i Asysty Rodzinnej MOPS – Bydgoszcz ul. Toruńska 272	- wszystkie pomieszczenia biurowe
5.	Rejonowy Ośrodek Pomocy Społecznej „Błonie" – Bydgoszcz ul. Broniewskiego 1	- wszystkie pomieszczenia biurowe
6.	Rejonowy Ośrodek Pomocy Społecznej „Szwederowo" – Bydgoszcz ul. Żwirki i Wigury 11	- wszystkie pomieszczenia biurowe
7.	Rejonowy Ośrodek Pomocy Społecznej „Śródmieście" – Bydgoszcz ul. Ogrodowa 9	- wszystkie pomieszczenia biurowe
8.	Rejonowy Ośrodek Pomocy Społecznej „Bartodzieje" – Bydgoszcz ul. Morska 2	- wszystkie pomieszczenia biurowe
9.	Rejonowy Ośrodek Pomocy Społecznej „Wyżyny" – Bydgoszcz ul. Kapuściska 10	- wszystkie pomieszczenia biurowe
10.	Rejonowy Ośrodek Pomocy Społecznej „Fordon" – Bydgoszcz ul. J. Porazińskiej 9	- wszystkie pomieszczenia biurowe
11.	Środowiskowy Dom Samopomocy „Niezapominajka" – Bydgoszcz ul. Ogrodowa 9	- wszystkie pomieszczenia biurowe
12.	Środowiskowy Dom Samopomocy „Bławatek" – Bydgoszcz ul. X. Dunikowskiego 2	- wszystkie pomieszczenia biurowe
13.	Środowiskowy Dom Samopomocy „Wrzos" – Bydgoszcz ul. Janosika 14	- wszystkie pomieszczenia biurowe
14.	Świetlica Środowiskowa „Nasz Dom" – Bydgoszcz ul. Kapuściska 10	- wszystkie pomieszczenia biurowe
15.	Świetlica Środowiskowa „Wodny Kraj" – Bydgoszcz ul. Toruńska 185	- wszystkie pomieszczenia biurowe
16.	Świetlica Środowiskowa „Grota" – Bydgoszcz ul. Świetlicowa 8	- wszystkie pomieszczenia biurowe
17.	Świetlica Środowiskowa „Marzenia" – Bydgoszcz ul. Smoleńska 43	- wszystkie pomieszczenia biurowe
18.	Świetlica Środowiskowa „Junior" – Bydgoszcz ul. Jodłowa 14	- wszystkie pomieszczenia biurowe
19.	Świetlica Środowiskowa „Puchatek" – Bydgoszcz ul. Przemysłowa 34	- wszystkie pomieszczenia biurowe
20.	Świetlica Środowiskowa „Dziecięcy Tygiel" – Bydgoszcz ul. Broniewskiego 1	- wszystkie pomieszczenia biurowe

I.2 Zbiory danych przetwarzanych w systemach informatycznych i opis struktury przetwarzanych danych osobowych

Zbiór danych osobowych	Program informatyczny służący do przetwarzania zbioru danych	Struktura danych osobowych	Wykaz pomieszczeń, w których przetwarzane są dane osobowe
- zbiór danych o pracownikach	**- program AgemaHR**	- PESEL/NIP, - imię i nazwisko - data i miejsce urodzenia, stan cywilny, dzieci, - płeć/adres/imię ojca i matki/nazwisko rodowe, obywatelstwo, - Nr D.O. i przez kogo wydany, - PIT, zarobki pracowników, - dane majątkowe, - karalność, - nieobecności w pracy, stan zdrowia, - wykształcenie	**MOPS:** - dyrektor (p. 27), - gł. księgowy (24), - kadry (p.41), - płace (p. 29),
	- program Infokonto	- PESEL/NIP, - imię, nazwisko, - data i miejsce ur. - adres zamieszkania, - dane majątkowe	**MOPS:** - dyrektor (p. 27), -gł. księgowy (p. 24), - DFK (p. 25), - DFK (p. 26), - KASA (p.1).
	- program Płatnik	- PESEL/NIP, - imię, nazwisko, - data i miejsce ur., - adres zamieszkania, - dane majątkowe, - Nr D.O. lub innego dowodu tożsamości	**MOPS:** - dyrektor (p. 27), - gł. księgowy (p. 24), - Zespół Kadr (p.41), - DFK - płace (p. 29), - DFK (p. 25), - DFK (p. 26), - KASA (p.1), - DRŚ (p. 47a), - DRON-Księgowość

- zbiór danych o podopiecznych pomocy społecznej	**-program„Płatnik"**	- PESEL/NIP, - imię, nazwisko, - data i miejsce ur., - adres zamieszkania, - dane majątkowe, - Nr D.O. lub innego dowodu tożsamości	**MOPS:** - KASA (p.1), - DRŚ (p. 47a), - DRON-wszystkie stanowiska, **ROPS – Ba** - sekcja świadczeń (p. 12), **ROPS – F** - sekcja świadczeń (p. 25), **ROPS – Szw** - sekcja świadczeń (p. 4), **ROPS – Bł** - sekcja świadczeń (p. 1), **ROPS – Śr** - sekcja świadczeń (p. 13 i 14), **ROPS – W** - sekcja świadczeń (p. 10).
	-program„Pomost"	- PESEL/NIP, - imię i nazwisko - data i miejsce urodzenia, stan cywilny, dzieci, - płeć/adres/imię ojca i matki/nazwisko rodowe, wykształcenie,obywatelstwo, - Nr D.O. i przez kogo wydany - dane majątkowe, - karalność, - stan zdrowia, - nałogi i uzależnienia, - leczenie specjalistyczne itp. - decyzje administracyjne.	**MOPS** **- DRŚ** - wszystkie stanowiska komputerowe, **ROPS – Śr** - wszystkie stanowiska komputerowe, **ROPS – Bł** - wszystkie stanowiska komputerowe, **ROPS – Ba** - wszystkie stanowiska komputerowe **ROPS – F** - wszystkie stanowiska komputerowe, **ROPS – Szw** - wszystkie stanowiska

			komputerowe, **ROPS – W** - wszystkie stanowiska komputerowe

I.3 Zbiory danych przetwarzanych tradycyjnie (papierowo)

Zbiór danych osobowych	Dokumentacja służąca do przetwarzania zbioru danych	Struktura danych osobowych	Wykaz pomieszczeń, w których przetwarzane są dane osobowe
- zbiór danych o pracownikach i podmiotach zewnętrznych	**akta osobowe**	- PESEL/NIP, - imię i nazwisko - data i miejsce urodzenia, stan cywilny, dzieci, - płeć/adres/imię ojca i matki/nazwisko rodowe, obywatelstwo, - Nr D.O. i przez kogo wydany, - PIT, zarobki pracowników, - dane majątkowe, - karalność, - nieobecności w pracy, stan zdrowia, - wykształcenie, - staż pracy, uzyskane kwalifikacje, - orzeczenia lekarskie, - dokumentacja ubezpieczeniowa itp.	**MOPS** - dyrektor - Zespół Kadr
	- Lista płac, **- Karta wynagrodzeń,** **- Roczna informacja o wynagrodzeniu (PIT),** **- zaświadczenia,** **- dokumentacja**	- PESEL/NIP, - imię, nazwisko, - data i miejsce ur., - adres zamieszkania, - dane majątkowe, - Nr D.O. lub innego dowodu tożsamości, - nieobecności w pracy, - zajęcia komornicze, - nagrody pieniężne, - dokumentacja ubezpieczeniowa, - zaświadczenia o zarobkach	**MOPS** - dyrektor, - Gł. Księgowy, - DFK; - Zespół Kadr

	ubezpieczeniowa	- itp.	
	- dokumentacja związana z realizacja ustawy Prawo zamówień publicznych, **- nadzorowanie systemu teleinformatycznego Ośrodka,** **- prowadzenie archiwizacji,** **- prowadzenie dokumentacji wykonywania kary ograniczenia wolności orzeczonej wyrokiem sadowym**	- dane osobowe podmiotów uczestniczących w przetargach, - dane osobowe zapisane w systemie teleinformatycznym, - zapisywanie danych osobowych i przechowywanie ich na kopiach zapasowych, - przechowywanie danych osobowych (w systemie papierowym) w archiwum zakładowym - dane osobowe osób wykonujących prace społeczne orzeczone wyrokiem sadowym	**MOPS** - dyrektor, - Zespół Prawny, - DOA
- zbiór danych o podopiecznych pomocy społecznej	**- dokumentacja osobowa podopiecznych pomocy społecznej,** **- dokumentacja w sprawach sądowych i administracyjnych pomocy społecznej,** **- decyzje administracyjne,** **- dokumentacja związana z realizacją zadań rodzinnej pieczy zastępczej,**	- PESEL/NIP, - imię i nazwisko - data i miejsce urodzenia, stan cywilny, dzieci, - płeć/adres/imię ojca i matki/nazwisko rodowe, wykształcenie,obywatelstwo, - Nr D.O. i przez kogo wydany - dane majątkowe, - karalność, - stan zdrowia, - nałogi i uzależnienia,	**MOPS** - dyrektor, - Zespół Prawny, - DRŚ, - DRON, - DRPZ, - DWR, - ZPS **- ROPS – Śr** - wszystkie stanowiska, **ROPS – Bł** - wszystkie stanowiska, **ROPS – Ba** - wszystkie stanowiska, **ROPS – F** - wszystkie stanowiska, **ROPS – Szw** - wszystkie stanowiska, **ROPS – W** - wszystkie stanowiska, **ŚDS – N** - wszystkie stanowiska, **ŚDS – B** - wszystkie

	- dokumentacja związana z realizacją pomocy osobom niepełnosprawnym, **- dokumentacja związana z realizacja zadań wsparcia rodziny i asysty rodzinnej,** **- dokumentacja związana z zadaniami realizacji świadczeń i pomocy instytucjonalnej**	- leczenie specjalistyczne itp. - decyzje administracyjne, - wywiady środowiskowe i alimentacyjne, - niepełnosprawność, - historia choroby, - zaświadczenia - skierowania do DPS, ZP-O, - windykacja należności, - dokumentacja związana z działaniami wobec osób i rodzin dotkniętych przemocą, - dokumentacja dzieci, korzystających ze świetlic środowiskowych, - dokumentacja uczestników ŚDS, - itd.	stanowiska, **ŚDS – W** - wszystkie stanowiska, **Świetlica „Nasz Dom"**-wszystkie stanowiska **Świetlica „Wodny Kraj"**-wszystkie stanowiska, **Świetlica „Grota"**-wszystkie stanowiska, **Świetlica „Marzenia"**-wszystkie stanowiska, **Świetlica „Junior"**-wszystkie stanowiska, **Świetlica „Puchatek"**-wszystkie stanowiska, **Świetlica „Dziecięcy Tygiel"**-wszystkie stanowiska
	- dokumentacja „Niebieska Karta"	- określona w ustawie z dnia 29 lipca 2005r. o przeciwdziałaniu przemocy w rodzinie (Dz.U. Nr 180, poz. 1493 z późn. zm.)	**j.w**
	- dokumentacja Kart DBF oraz Kart DBT – ewidencja danych świadczeniobiorców	- określona przepisami: 1) ustawy o pomocy społecznej, 2) ustawy o zasiłkach rodzinnych, 3) ustawy o ochronie zdrowia psychicznego, 4) ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych	**j.w.**

I.4 Środki techniczne i organizacyjne w przetwarzaniu danych

I.4.1 Cele i zasady funkcjonowania polityki bezpieczeństwa

§ 1

1. Celem Polityki Bezpieczeństwa jest zapewnienie ochrony DANYCH OSOBOWYCH przetwarzanych w celach określonych w art. 27 ust. 2 pkt 7 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r. Nr 101, poz. 926, z późn. zm.) przetwarzanych przez Ośrodek, przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi, świadomymi lub nieświadomymi.

2. Polityka Bezpieczeństwa obowiązuje wszystkich pracowników Ośrodka oraz dostawców, podmiotów współpracujących na podstawie umów cywilnoprawnych, mających jakikolwiek kontakt z danymi osobowymi, objętymi ochroną.

3. Realizując Politykę Bezpieczeństwa informacji, zapewnia się ją poprzez:
   a) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
   b) integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
   c) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
   d) rozliczalność – możliwość jednoznacznego przypisywania działań poszczególnym osobom,
   e) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
   f) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
   g) niezawodność – zamierzone zachowania i skutki są spójne.

4. Polityka Bezpieczeństwa informacji w Ośrodku, ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:
   1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Ośrodkowi;
   2) naruszeń przepisów prawa oraz innych regulacji;
   3) utraty lub obniżenia reputacji Ośrodka;
   4) strat finansowych ponoszonych w wyniku nałożonych kar;
   5) zakłóceń organizacji pracy, spowodowanych nieprawidłowym działaniem systemów.

5. Realizując Politykę Bezpieczeństwa w zakresie ochrony danych osobowych, Ośrodek dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby te dane były:
   - przetwarzane zgodnie z prawem,
   - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane ich dalszemu przetwarzaniu, niezgodnemu z tymi celami,
   - merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
   - przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

I.4.2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§ 2

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób nie zapewniający ochrony interesów osób, których te dane dotyczą, grozi odpowiedzialność karna, wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza, na zasadach określonych w kodeksie pracy.

§ 3

Administrator Danych Osobowych (ADO) – Dyrektor Ośrodka:

1. Formułuje i wdraża warunki techniczne i organizacyjne, służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez nieuprawnioną osobę, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
2. Decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
3. Odpowiada za zgodne z prawem przetwarzanie danych osobowych w Ośrodku.

§ 4

Administrator Bezpieczeństwa Informacji (ABI) – pracownik Ośrodka, wyznaczony przez Dyrektora:

1. Egzekwuje zgodne z prawem przetwarzanie danych osobowych w Ośrodku, w imieniu **ADO**,
2. Wydaje upoważnienie do przetwarzania danych osobowych, określając w nich zakres i termin ważności – wzór upoważnienia określa załącznik Nr 1,
3. Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa załącznik Nr 2,
4. Ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa załącznik Nr 3,
5. Określa potrzeby w zakresie stosowanych w Ośrodku zabezpieczeń, wnioskuje do **ADO** o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia,
6. Udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
7. Bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w Ośrodku i zapewnia odpowiedni poziom przeszkolenia w tym zakresie,
8. Nadzoruje dokonywanie zgłoszeń zbioru danych osobowych do rejestrów GIODO. Zgłoszeniu podlegają takie usystematyzowane zestawy danych, które są zbiorami danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych,
9. Kontroluje, **minimum 1 raz w miesiącu** i sporządza z tej czynności protokół, z tworzenia i przechowywania kopii zapasowych danych osobowych przechowywanych w systemie informatycznym Ośrodka,

10. Nadzoruje i kontroluje sposób zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe oraz pomieszczeń serwerowni we wszystkich komórkach organizacyjnych Ośrodka,
11. Administrator Bezpieczeństwa Informacji i Administrator Systemów Informatycznych przeprowadzają okresowe, **minimum raz na 3 miesiące**, analizy ryzyka dla poszczególnych systemów
12. Na koniec roku kalendarzowego, **do dnia 31 grudnia każdego roku**, przedkłada Administratorowi Danych Osobowych (ADO), **pisemną informację, o stanie bezpieczeństwa danych osobowych w Ośrodku.**

§ 5

Administrator Systemu Informatycznego (ASI) – pracownik Ośrodka wyznaczony przez Dyrektora:

1. Zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym, zgodnie z wymogami prawa i wskazówkami ABI,
2. Doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
3. Przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
4. Nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
5. Zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
6. Prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji, zawierających dane osobowe,

§ 6

Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez ABI:

1. Chroni prawo do prywatności osób fizycznych, powierzających Ośrodkowi swoje dane osobowe, poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Ośrodka,
2. Zapoznaje się z zasadami określonymi w Polityce Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Ośrodka i składa oświadczenie o znajomości tych przepisów.

I.4.3 Zasady udzielania dostępu do danych osobowych

§ 7

1. Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Ośrodku, Polityce Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym. Osoba zaznajomiona z zasadami ochrony danych, potwierdza to w pisemnym oświadczeniu,

2. Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ABI,

I.4.4 Udostępnianie i powierzanie danych osobowych

§ 8

Dane osobowe mogą być udostępniane osobom i podmiotom, zgodnie z przepisami prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 9

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:
- adresat wniosku (administrator danych),
- wnioskodawca,
- podstawa prawna (wskazanie potrzeby),
- wskazanie przeznaczenia,
- zakres informacji.

§ 10

Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 11

Powierzenie danych może nastąpić wyłącznie w formie pisemnej umowy, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 12

Każda osoba fizyczna, której dane są przetwarzane w Ośrodku, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 13

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ABI, udzielając informacji o zawartości zbioru danych na piśmie, zgodnie ze wzorem załącznika Nr 4.

I.4.5 Bezpieczeństwo w przetwarzaniu danych osobowych, w formie tradycyjnej

§ 14

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Każdorazowe opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych, musi być poprzedzone przeniesieniem zbioru do odpowiednio zabezpieczonego miejsca i zamknięte na klucz.

§ 15

Klucze do szaf, w których przechowywane są dane osobowe, mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.

§ 16

Klucze od pomieszczeń, w których przechowywane są dane osobowe, powinny być przechowywane w odpowiednio zabezpieczonym miejscu i kontrolowane.

§ 17

Przed opuszczeniem przez pracownika pomieszczenia, w którym przechowywane są dane osobowe, zbiory danych osobowych powinny być umieszczone w odpowiednio zabezpieczone miejsca (szafy). Zasadą powinno być tz. „czyste biurko".

§ 18

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Ośrodku, a upoważnione do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów, powinno odbywać się po konsultacji z ABI i uzyskaniu upoważnienia przez tą osobę.

§ 19

Zabrania się wynoszenia poza budynek, w którym przetwarzane są dane osobowe, zbiorów przetwarzanych przez Ośrodek i jego komórki organizacyjne oraz kopiowania ich do innych celów, niż służbowe.

I.4.6 Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

§ 20

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w *Instrukcji zarządzania systemem informatycznym*, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Ośrodka.

I.5 Analiza ryzyka związanego z przetwarzaniem danych osobowych

I.5.1 Identyfikacja zagrożeń

§ 21

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
dane przetwarzane w sposób tradycyjny	– oszustwo, kradzież, sabotaż; – zdarzenia losowe (powódź, pożar); – zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); – niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; – pokonanie zabezpieczeń fizycznych; – podsłuchy, podglądy; – ataki terrorystyczne; – brak rejestrowania udostępniania danych; – niewłaściwe miejsce i sposób przechowywania dokumentacji;
dane przetwarzane w systemach informatycznych	– nie przydzielenie użytkownikom systemu informatycznego identyfikatorów; – niewłaściwa administracja systemem; – niewłaściwa konfiguracja systemu; – zniszczenie (sfałszowanie) kont użytkowników; – kradzież danych kont; – pokonanie zabezpieczeń programowych; – zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); – niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; – zdarzenia losowe (powódź, pożar); – niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych; – naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione; – przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci; – przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci; – przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych – brak rejestrowania zdarzeń tworzenia lub modyfikowania danych;

I.5.2 Sposób zabezpieczenia danych

§ 22

FORMA PRZETWARZANIA DANYCH	STOSOWANE ŚRODKI OCHRONY
dane przetwarzane w sposób tradycyjny	– przechowywanie danych w pomieszczeniach zamykanych na zamki patentowe; – przechowywanie danych osobowych w szafach zamykanych na klucz; – zastosowanie czujników ruchu informujących firmę ochroniarską o nieautoryzowanym wejściu do budynku; – zastosowanie monitoringu wizyjnego regulującego gospodarkę kluczami; – przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez ABI; – zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania;
dane przetwarzane w systemach informatycznych	– kontrola dostępu do systemów; – zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; – stosowanie ochrony zasilania; – systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; – składowanie danych sensytywnych oraz nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach; – zabezpieczenie pomieszczenia serwerowni; – przydzielenie pracownikom indywidualnych kont użytkowników i haseł; – stosowanie indywidualnych haseł logowania do poszczególnych programów; – właściwa budowa hasła;

I.5.3 Określenie wielkości ryzyka

§ 23

Poziom ryzyka naruszenia bezpieczeństwa danych w Ośrodku, ze względy na ilość przetwarzanych danych osobowych oraz fakt, że przetwarzanie tych danych odbywa się w budynkach zlokalizowanych w różnych regionach Miasta Bydgoszczy, jest wysoki. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów i kategorii danych osobowych.

I.5.4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§ 24

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa.

Administrator Bezpieczeństwa Informacji i Administrator Systemów Informatycznych przeprowadzają okresowe, **minimum raz na 3 miesiące**, analizy ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

Załącznik Nr 2
do Zarządzenia Nr 91 /2012
Dyrektora Miejskiego Ośrodka
Pomocy Społecznej w Bydgoszczy
z dnia 5 grudnia 2012r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

II.1 Procedury nadawania i zmiany uprawnień do przetwarzania danych w systemie informatycznym

§ 1

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z następującymi dokumentami:

1) ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2002r. Nr 101, poz. 926 z późn. zm.),
2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100, poz. 1024),
3) niniejszą polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym.

2. Zapoznanie się z powyższymi dokumentami, użytkownik systemu potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik Nr 3 do niniejszej instrukcji.

§ 2

Przetwarzania danych osobowych może dokonać jedynie użytkownik systemu, upoważniony przez administratora danych osobowych (ABI). Wzór upoważnienia stanowi załącznik Nr 1 do niniejszej instrukcji.

§ 3

ABI prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych, według wzoru stanowiącego załącznik Nr 2, niniejszej instrukcji.

§ 4

1. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników, odpowiada ASI,
2. ASI nadaje uprawnienia w systemie informatycznym, na podstawie upoważnienia nadanego pracownikowi przez ABI,

3. Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywaniu konta danego użytkownika i ulega ono dezaktywacji w celu zachowania historii jego aktywności

§ 5

Osoby dopuszczone do przetwarzania danych osobowych, zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

II.2 Zabezpieczenie danych w systemie informatycznym

§ 6

Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe, zapewniają zasilacze UPS.

§ 7

W przypadkach awaryjnych, takich jak nagły brak zasilania, ciągłość funkcjonowania systemu informatycznego podtrzymuje bateria zasilająca serwera. W czasie pracy baterii zasilającej ASI dokonuje oceny sytuacji i podejmuje wszelkie niezbędne kroki w celu zachowania integralności danych oraz przywrócenia normalnego funkcjonowania systemu.

§ 8

1. Oprogramowanie wykorzystywane do przetwarzania danych osobowych, posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system,
2. Hasła do systemu stacji roboczych, kontrolowanych przez kontroler domeny (PDC), mają długość przynajmniej 8 znaków (duże i małe litery oraz cyfry i znaki specjalne) i okres ważności ustawiony na nie dłużej, niż 1 miesiąc,
3. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.

§ 9

W przypadku utracenia hasła, użytkownik ma obowiązek skontaktować się z ASI, celem uzyskania nowego hasła.

§ 10

System informatyczny przetwarzający dane osobowe, musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych osobowych. W szczególności zapis ten powinien obejmować:
- rozpoczęcie i zakończenie pracy przez system użytkownika systemu,
- operacje wykonywane na przetwarzanych danych,

- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

§ 11

System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych, z uwzględnieniem:
- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

§ 12

1. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości, przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania") na każdym komputerze, na którym przetwarzane są dane osobowe.

Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada ASI.

2. **Pracownicy użytkujący komputery przenośne, a pracujący na danych osobowych, zabronione jest wynoszenie ich poza miejsce pracy. W przypadku takiej potrzeby, muszą uzyskać zgodę administratora danych (ADO) i stosować środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.**

II.3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym

§ 13

W celu rozpoczęcia pracy w systemie informatycznym, użytkownik wykonuje następujące czynności:
1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (autoryzacja użytkownika w bazie usług katalogowych),
2) loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.

§ 14

W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym, należy uniemożliwić osobom postronnym, korzystanie z systemu informatycznego, poprzez wylogowanie się z systemu lub uruchomienie się wygaszacza ekranu, chroniony hasłem.

§ 15

W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba, należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor w sposób uniemożliwiający wgląd w wyświetlaną treść.

§ 16

Użytkownik wyrejestruje się z systemu informatycznego przed wyłączeniem stacji komputerowej, poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.

§ 17

Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:
- podejrzenia naruszenia bezpieczeństwa systemu;
- braku możliwości zalogowania się użytkownika na jego konto;
- stwierdzenia fizycznej ingerencji w przetwarzane dane;
- stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

§ 18

1. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
- nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);
- wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);
- różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);
- inne nadzwyczajne sytuacje;
2. Pomieszczenie serwerowni powinno być szczególnie reglamentowane i chronione (zamykane). **Wejście osób postronnych jest zabronione**. Każdorazowe wejście osób upoważnionych, powinno być odnotowane w zeszycie wejść, który znajduje się u kierownika komórki organizacyjnej, w których się one znajdują.

II.4 Tworzenie kopii zapasowych

§ 19

Kopie zapasowe, zawierające zbiory danych osobowych wykonywane są automatycznie, dedykowanym oprogramowaniem, po zakończeniu pracy Ośrodka, od poniedziałku do piątku każdego tygodnia. Kopiowana jest baza programu „Pomost" oraz „Płatnik". Po utworzeniu kopii, wysyłana jest ona na serwer Ośrodka i tam przechowywana.

Kopie dokumentów na dysku wspólnym, wykonywane są raz w tygodniu oraz przesyłane na serwer Ośrodka. Po utworzeniu kopii, generowany jest raport z przebiegu kopiowania oraz jego poprawności.

Za wykonywanie kopii odpowiada informatyk Ośrodka, obsługujący dany rejon.

§ 20

Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa, niszczy się trwale w sposób mechaniczny.

II.5 Udostępnienie danych

§ 21

Dane osobowe przetwarzane w systemach informatycznych, zgodnie z art. 27 ust. 2 pkt 7 ustawy, mogą być wydane osobom, których dane dotyczą, jedynie na ich pisemny wniosek, lub pisemny wniosek osoby upoważnionej na piśmie przez zainteresowanego. Wzór wniosku stanowi załącznik Nr 4 niniejszej instrukcji.

II.6 Przeglądy i konserwacje systemów

§ 22

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Ośrodka (ASI) lub przez upoważnionych przedstawicieli serwisu.

§ 23

Prace wymienione w § 22, powinny uwzględniać wymagany poziom zabezpieczenia danych osobowych przed dostępem do nich osób nieupoważnionych.

§ 24

1. Naprawa sprzętu komputerowego, użytkowanego w systemie, poza siedzibą Ośrodka, musi zostać poprzedzona usunięciem z twardego dysku wszelkich aplikacji przetwarzających i zawierających dane o charakterze osobowym lub całego twardego dysku;
2. ASI jest odpowiedzialny za stworzenie kopii tej bazy, która jest przechowywana przez ASI, w zabezpieczonym pomieszczeniu, do czasu powrotu sprzętu z serwisu.
3. Po powrocie z serwisu sprzętu komputerowego, ASI ponownie instaluje bazę danych, a jej kopia zostaje zniszczona.
4. W przypadku oddania sprzętu do serwisu, bez twardego dysku, ASI przechowuje dysk w odpowiednim pomieszczeniu, aż do jego powrotu z serwisu.

II.7 Niszczenie wydruków i nośników danych

§ 25

1. Wszelkie wydruki z systemów informatycznych, zawierające dane osobowe, przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek;
2. Niszczenie zapisów na nośnikach danych, powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika;
3. Uszkodzone nośniki danych, przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce;

Załącznik Nr 3
do Zarządzenia Nr 91 /2012
Dyrektora Miejskiego Ośrodka
Pomocy Społecznej w Bydgoszczy
z dnia 5 grudnia 2012r.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

III.1 Istota naruszenia danych osobowych

§ 26

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
- nieautoryzowany dostęp do danych;
- nieautoryzowane modyfikacje lub zniszczenie danych;
- udostępnienie danych nieautoryzowanym podmiotom;
- nielegalne ujawnienie danych;
- pozyskanie danych z nielegalnego źródła.

III.2 Procedura postępowania w sytuacji naruszenia polityki bezpieczeństwa

§ 27

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym ABI lub inną upoważnioną osobę.
2. ASI (lub upoważniona osoba) w porozumieniu z ABI po otrzymaniu powiadomienia:

a) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
b) sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
c) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
d) sprawdza zawartość zbioru danych osobowych,
e) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.

3. W przypadku stwierdzenia naruszenia zabezpieczeń danych administrator:

a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),
b) w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
c) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,

d) niezwłocznie przywraca prawidłowy stan działania systemu,
e) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
f) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) ABI przekazuje administratorowi danych osobowych.
5. ABI, w porozumieniu z administratorem danych osobowych, podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

a) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,
b) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągnięcie konsekwencji przewidzianych prawem,
c) jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, zawiadamia organy ścigania.

§ 28

ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego załącznik nr 5 i przekazuje go ADO.

§ 29

ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

III.3 Sankcje karne

§ 30

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

§ 31

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Załączniki

Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych

Załącznik nr 2 – Rejestr osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 3 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych

Załącznik nr 4 – Informacja o zawartości zbioru danych

Załącznik nr 5 – Raportu z naruszenia bezpieczeństwa danych osobowych

Załącznik Nr 1
do „Polityki bezpieczeństwa

Bydgoszcz, dnia ..... r.

.....

UPOWAŻNIENIE nr ...../ do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) upoważniam Panią/Pana .... zatrudnioną (ego) w Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy,

na stanowisku .....do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w okresie od dnia ..... 20.... r. do .....

w zakresie określonym obowiązkach służbowych.

Wyżej wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Ośrodku.

.....
(podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 2
do „Polityki bezpieczeństwa

Bydgoszcz , dnia ..... r.

.....

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Identyfikator użytkownika*	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień i podpis ABI	Data odebrania uprawnień i podpis ABI	Uwagi

* Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie

Załącznik Nr 3
do „Polityki bezpieczeństwa

..... Bydgoszcz, dnia ..... r.
(imię i nazwisko)

.....
(stanowisko)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy , jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Ośrodku zasadach dotyczących przetwarzania danych osobowych, określonych w „Polityce bezpieczeństwa informacji w Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy"
i zobowiązuję się ich przestrzegać.

W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Ośrodku

Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926 z późn. zm.) oraz Rozporządzenia MSWiA 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). Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....
(podpis pracownika)

Załącznik Nr 4
do „Polityki bezpieczeństwa

Bydgoszcz, dnia ..... r.

.....

.....
(imię i nazwisko)

.....

.....
(adres)

INFORMACJA
o zawartości zbioru danych osobowych

W związku z Pani/Pana wnioskiem z dnia ..... r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy
działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe: .....

.....

Powyższe dane przetwarzane są w Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy w celu ..... z zachowaniem wymaganych zabezpieczeń i zostały uzyskane ..... (podać sposób).

Powyższe dane nie były / były udostępniane .....
(podać komu) w celu ..... (podać cel przekazania danych).

Zgodnie z rozdziałem 4 Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

.....
(podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 5
do „Polityki bezpieczeństwa

Bydgoszcz, dnia ..... r.

.....

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Miejskim Ośrodku Pomocy Społecznej w Bydgoszczy

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

.....
(podpis Administratora Bezpieczeństwa Informacji