Zarządzenie Nr 2 /2014
Dyrektora Domu Pomocy Społecznej
Im. W. Michelisowej w Lublinie
z dnia 6 marca 2014r.

w sprawie ochrony danych osobowych w Domu Pomocy Społecznej im W. Michelisowej w Lublinie

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz, U. z 2002r. Nr 101 poz. 926 z późn.zm.), rozporządzenia 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. Nr100 poz. 1024) oraz § 8 ust. 7 regulaminu organizacyjnego Domu Pomocy Społecznej im. W. Michelisowej w Lublinie stanowiącego załącznik do zarządzenia Nr 29 / 3 / 2013 Prezydenta Miasta Lublin z dnia 12.03.2013r. w sprawie przyjęcia regulaminu organizacyjnego Domu Pomocy Społecznej im. W. Michelisowej w Lublinie zarządzam, co następuje:

§1

1. Wyznaczam Pana Krzysztofa Błażuckiego jako administratora bezpieczeństwa informacji zwanego dalej ABI w Domu Pomocy Społecznej im. W. Michelisowej w Lublinie, zwanym dalej „Domem"
2. Zadaniem ABI jest nadzór nad przestrzeganiem zasad ochrony przetwarzania danych osobowych, a w szczególności nadzór nad zabezpieczeniami danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. W zakresie realizowanych zadań ABI jest upoważniony do:
   - przeprowadzania okresowych i doraźnych kontroli w zakresie przestrzegania zasad bezpieczeństwa danych osobowych oraz w celu identyfikacji potencjalnych zagrożeń,
   - podejmowania działań i zaleceń w przypadku naruszenia bezpieczeństwa danych osobowych,
   - współdziałania z osobami upoważnionymi do dostępu do zbiorów danych osobowych.
4. ABI określa hasła użytkowania komputerów do przetwarzania danych osobowych i zmienia je w razie potrzeby.
5. Upoważniam kierowników komórek organizacyjnych Domu do wykonywania zadań administratora danych osobowych, w odniesieniu do danych osobowych przetwarzanych w tych komórkach organizacyjnych

§2

1. Do przetwarzania danych osobowych dopuszcza się wyłącznie osoby posiadające stosowne upoważnienie.
2. Wzór upoważnienia stanowi Zał. Nr 1 do zarządzenia. Wzór oświadczenia pracownika stanowi Zał. Nr 2 do zarządzenia.
3. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi inspektor ds. pracowniczych

4. Ewidencja o której mowa w ust.3 zawiera:
   1) imię i nazwisko osoby upoważnionej,
   2) datę nadania i ustania upoważnienia oraz zakres upoważnienia do przetwarzania danych osobowych,

§3

1. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są:
   1) siedziby komórek organizacyjnych budynku Domu Pomocy Społecznej im. W. Michelisowej w Lublinie – a w szczególności – Gabinet Dyrektora Domu, i jego zastępcy, sekretariat, część administracyjna budynku, księgowość, pomieszczenia zespołu opiekuńczo – pielęgnacyjnego i terapeutyczno - rehabilitacyjnego.
2. Ustala się procedurę rozpoczęcia i zakończenia pracy na stanowiskach, na których przetwarzane są dane osobowe w systemie komputerowym:
   1) ustawienie monitorów w sposób uniemożliwiający dostęp do informacji osobom nieuprawnionym,
   2) uruchomienie komputera odpowiednim hasłem,
   3) w czasie przerw w pracy zastosowanie wygaszacza ekranu,
   4) upewnienie się, czy dane zostały zarejestrowane,
   5) zakończenie pracy związanej z przetwarzaniem danych powinno odpowiadać wszystkim regułom bezpieczeństwa informacji.
3. Kopie informatyczne, wydruki wykonywane są w miarę potrzeb.
4. Nośniki danych oraz wydruki, nie przeznaczone do udostępniania przechowywane są w specjalnie zamykanych szafkach, do których dostęp mają tylko osoby uprawnione.
5. Wszelkie awarie systemu oraz naruszenia bezpieczeństwa wymagają natychmiastowego powiadomienia ABI lub ADO
6. Polityka bezpieczeństwa informacji w zakresie przetwarzania danych osobowych zawarta jest Zał. Nr 3 do zarządzenia.
7. Instrukcję zarządzania systemem informatycznym stanowi Zał. Nr 4 do zarządzenia.

§4

1. Wykaz zbiorów danych osobowych stanowią:
   1) Akta osobowe pracowników i mieszkańców;
   2) Dokumentacja polityki kadrowej, w tym dane zbierane w procesie rekrutacji;
   3) Ewidencje w sprawach pracowniczych;
   4) Listy płac;
   5) Deklaracje podatkowe, ubezpieczeniowe pracowników;
   6) Dane gromadzone w systemie zamówień publicznych;
   7) Rejestr osób dopuszczonych do przetwarzania danych osobowych;
   8) Dokumentacja medyczna;
   9) Archiwum
2. Dane w/w są przetwarzane w Domu w systemie informatycznym, w komputerach ewidencjonowanych w spisie inwentarzowym jednostki.
3 Wykaz programów dopuszczonych do używania na poszczególnych stanowiskach pracy stanowi Zał. Nr 5 do zarządzenia.

4 Wprowadza się bezwzględny zakaz użytkowania programów zainstalowanych nielegalnie.
5. Wprowadza się bezwzględny zakaz korzystania z Internetu w celach nie związanych bezpośrednio z zakresem obowiązków lub poleceniami przełożonych.
6. Oświadczenie pracownika w sprawie korzystania z sieci komputerowej Domu Pomocy Społecznej im. W. Michelisowej w Lublinie stanowi Załącznik Nr 6 do zarządzenia

§5

1. Wykonanie zarządzenia powierzam ABI, kierownikom komórek organizacyjnych Domu oraz innym pracownikom upoważnionym do przetwarzania danych osobowych.
2. Nadzór nad realizacją zarządzenia powierzam zastępcy dyrektora.
3. Odebranie oświadczeń od pracowników, gromadzenie ich w aktach osobowych powierzam pracownikowi na stanowisku ds. pracowniczych.
4. Dotychczasowe upoważnienia i oświadczenia pracowników złożone przed wejściem w życie zarządzenia pozostają w mocy.

§6

Tracą moc zarządzenia Dyrektora Nr 19/2004 z dnia 2.11.2004r. w sprawie: ochrony danych osobowych w Domu Pomocy Społecznej im. W. Michelisowej w Lublinie Nr 4/2008 z dnia 11 lutego 2008r w sprawie programów komputerowych użytkowanych przez pracowników Domu w celach służbowych Nr 14/2013 z dnia 23 września 2013r w sprawie uzupełnienia instrukcji zarządzania systemem informatycznym.

§ 7

Zarządzenie obowiązuje od dnia podpisania.

Załącznik Nr 1 - wzór upoważnienia do dostępu i przetwarzania danych osobowych
Załącznik Nr 2 - wzór oświadczenia pracownika
Załącznik Nr 3 - polityka bezpieczeństwa informacji w zakresie przetwarzania danych osobowych
Załącznik Nr 4 - instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
Załącznik Nr 5 - wykaz programów komputerowych dopuszczonych do używania na poszczególnych stanowiskach pracy
Załącznik Nr 6 - Oświadczenie pracownika w sprawie korzystania z sieci komputerowej

Dyrektor D.P.S
/-/
mgr Jolanta Ślązak-Chabros

Zał. Nr 1 do Zarządzenia Nr 2 /2014
Dyrektora Domu Pomocy Społecznej
Im. W. Michelisowej w Lublinie
z dnia 6 marca 2014.
w sprawie ochrony danych osobowych
w Domu Pomocy Społecznej
im. W. Michelisowej w Lublinie

Lublin,dn……..

U P O W A Ż N I E N I E

do dostępu i przetwarzania danych osobowych

Upoważniam Pana/Panią ..... Nr Pesel ..... do przetwarzania danych osobowych na potrzeby Domu Pomocy Społecznej Im. W. Michelisowej w Lublinie w zakresie .....
.....
.....

Upoważnienie ważne jest w okresie wykonywania pracy w Domu Pomocy Społecznej im. W. Michelisowej w Lublinie.

Pouczenie:
Osoba upoważniona obowiązana jest do zachowania w tajemnicy informacji uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych oraz sposobu ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Naruszenie obowiązku zabezpieczenia danych osobowych powoduje

odpowiedzialność karną zgodnie z Rozdziałem 8 ustawy z dnia 29.08.1997r

o ochronie danych osobowych (Dz.U. z 2002r. Nr 101, poz. 926, z późn.zm.)

Przyjąłem/Przyjęłam do wiadomości i stosowania

.....
data i podpis pracownika (innej osoby upoważnionej)

sporządzono w 2 egzemplarzach:
1- dla pracownika
2- akta osobowe

Zał. Nr 2 do Zarządzenia Nr 2 /2014
Dyrektora Domu Pomocy Społecznej
Im. W. Michelisowej w Lublinie
z dnia ...6 marca 2014..r.
w sprawie ochrony danych osobowych
w Domu Pomocy Społecznej
im. W. Michelisowej w Lublinie

Lublin dn, ...

.....
imię i nazwisko pracownika

.....
seria i nr dowodu osobistego

O Ś W I A D C Z E N I E

Oświadczam i zobowiązuję się do:

- zachowania tajemnicy danych osobowych do przetwarzania, których zostałem(am) upoważniony(a),
- nie ujawniania żadnych wiadomości z tym związanych,
- ochrony danych przed udostępnieniem osobom nie upoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.

Jednocześnie oświadczam, że znane mi są przepisy dotyczące ochrony danych osobowych.

Świadomy(a) odpowiedzialności karnej wynikającej z przekroczenia w/w reguł, potwierdzam swoją wolę własnoręcznym podpisem.

.....
data i podpis pracownika

Zaświadczam o przeszkoleniu stanowiskowym Panią / Pana.....
W zakresie ochrony danych osobowych zgodnie z obowiązującym zarządzeniem Dyrektora

Lublin dnia .....

.....
Administrator Bezpieczeństwa Informacji

Załącznik nr 3 do *Zarządzenia* Nr 2 /2014
Dyrektora Domu Pomocy Społecznej
Im. W. Michelisowej w Lublinie
z dnia 6 marca.... 2014r.
w sprawie ochrony danych osobowych
w Domu Pomocy Społecznej
im. W. Michelisowej w Lublinie

POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

W DOMU POMOCY SPOŁECZNEJ IM. W. MICHELISOWEJ W LUBLINIE

I. Postanowienia ogólne

§1.

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Domu informacji zawierających dane osobowe.

§2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. Komórka organizacyjna - odpowiednio komórki organizacyjne, o których mowa w regulaminie organizacyjnym Domu;
2. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
3. Przetwarzanie danych osobowych - gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych;
4. Użytkownik - osoba upoważniona do przetwarzania danych osobowych;
5. Administrator systemu - osoba upoważniona do zarządzania systemem informatycznym,
6. System informatyczny - system przetwarzania danych w Domu - wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
7. Zabezpieczenie systemu informatycznego - należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. Definicja bezpieczeństwa informacji

§3.

1. Utrzymanie bezpieczeństwa przetwarzanych przez Dom informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) Poufność informacji - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji;
   2) Integralność informacji - rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
   3) Dostępność informacji – rozumiana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   4) Zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

III. Zakres

§ 4

1. W systemie informacyjnym Domu przetwarzane są informacje służące do wykonywania zadań statutowych.
2. Informacje te są przetwarzane zarówno w postaci tradycyjnej jak i elektronicznej.

§ 5

Politykę Bezpieczeństwa stosuje się do danych osobowych wymienionych w § 4 ust. 1 zarządzenia.

§ 6

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Domu w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz tradycyjnych , w których przetwarzane są informacje podlegające ochronie;
   2) informacji będących własnością Domu lub jego kontrahentów o ile zostały przekazane na podstawie umów,
   3) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, praktykantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

§7

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. Struktura dokumentów polityki bezpieczeństwa informacji

1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z :

1) Polityki Bezpieczeństwa Informacji, stanowiącego Zał. Nr 3 do zarządzenia.
2) Instrukcji zarządzania systemem informatycznym w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, stanowiącej Zał. Nr 4 do zarządzenia.

V. Dostęp do informacji

§ 9

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają zapoznaniu się z niniejszym zarządzeniem.

§10

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§11

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.

VI. Zarządzanie danymi osobowymi

§12

Administratorem danych osobowych Domu jest Dyrektor Domu.

§13

Za bezpieczeństwo danych osobowych Domu, odpowiadają:
1) Administrator danych osobowych - Dyrektor Domu;
Z-ca Dyrektora –sprawujący nadzór nad realizacją zarządzenia Dyrektora Domu w sprawie ochrony danych osobowych
2) Administrator Bezpieczeństwa Informacji Domu;
3) Kierownicy komórek organizacyjnych Domu;

§14

1. Obowiązki wynikające z ustawy o ochronie danych osobowych Dyrektor Domu powierza Kierownikom komórek organizacyjnych Domu w zakresie podległych im pracowników oraz ABI.
2. Kierownicy komórek organizacyjnych Domu odpowiadają za realizację wymagań obowiązujących przepisów prawa, dotyczących ochrony danych osobowych, z obowiązkiem współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie swoich właściwości;
3 Z-ca Dyrektora i Kierownicy komórek organizacyjnych Domu zobowiązani są do zapoznania podległych pracowników z treścią ustawy z dnia 29 sierpnia 1997 r.

4 o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), i zarządzeniem wewnętrznym Dyrektora w tym zakresie.

§15

Ochrona zasobów danych osobowych Domu jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników Domu.

VII. Przetwarzanie danych osobowych

§16

Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

§17

Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów przetwarzania.

§18

Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

VIII. Archiwizowanie informacji zawierających dane osobowe

§19

Zasady archiwizacji i brakowania dokumentów reguluje Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikacji i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. Nr 167, poz. 1375) oraz aktualne zarządzenie Dyrektora Domu dotyczące instrukcji archiwalnej.

Załącznik nr 4 do *Zarządzenia* Nr2 /2014
Dyrektora Domu Pomocy Społecznej
im. W. Michelisowej w Lublinie
z dnia 6 marca.. 2014r.
w sprawie ochrony danych osobowych
w Domu Pomocy Społecznej
im. W. Michelisowej w Lublinie

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie 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) ustalam:

1. **Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.**

Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych. Upoważnienie nadaje i odwołuje Dyrektor Domu. Upoważnienie i jego odwołanie sporządzane są na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden przeznaczony jest dla osoby, której nadano lub odebrano upoważnienie, drugi do przechowywania w aktach tej osoby. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do zarządzenia.

Upoważnienia do przetwarzania danych osobowych rejestrowane są w rejestrze osób upoważnionych do przetwarzania danych osobowych prowadzonym na stanowisku pracy ds. pracowniczych..

2. **Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem**

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem. W Domu Pomocy Społecznej obowiązują następujące zasady tworzenia hasła:

- hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
- hasło musi składać się z co najmniej 6 znaków,
- hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
- hasło nie może być jednakowe z identyfikatorem użytkownika,
- hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy.

W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora danych.

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło. Hasła użytkowników systemu przechowywane są w zapieczętowanych kopertach w metalowej szafie w pomieszczeniu kasy przez Administratora Bezpieczeństwa Informacji.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić administratora danych.

Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych, wyłączyć monitor lub włączyć wygaszacz ekranu.

Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest informatyk.. Również ta osoba odpowiedzialna jest za sporządzanie kopii zapasowych danych.

Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe

nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych".

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach . stanowiących obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych", w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

W przypadku uszkodzenia lub zużycia nośnika informacji zwierającego dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

6. **Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych**

Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.

Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być, jeżeli jest to możliwe ze względów technicznych zainstalowanie oprogramowania antywirusowego. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

7. **Instrukcja alarmowa dotycząca bezpieczeństwa informatycznego.- zał. Nr 1**
8. **Instrukcja postępowania z danymi z wizyjnego monitoringu.- zał. Nr 2**
9. **Instrukcja korzystania z kart Pekaobiznes. – zał. Nr 3**
10. **Zasady prowadzenia kart sprzętu elektronicznego Domu**

Wprowadza się obowiązek wprowadzenia przez informatyka Domu kart sprzętu elektronicznego Domu tj komputerów, drukarek, kserokopiarek, skanerów.

Karta sprzętu zawiera w szczególności Nw pozycje:

1. Nazwa sprzętu i numer inwentarzowy
2. Data zakupu , nr faktury
3. Imię i nazwisko użytkownika sprzętu
4. Data rozpoczęcia użytkowania
5. Wykaz oprogramowania – data zakupu , nr faktury
6. Wykaz wykonanych istotnych czynności technicznych min instalacja oprogramowania.

Karta podlega uzgodnieniu z działem A-G i F-K Domu na koniec każdego roku kalendarzowego.

11. **Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych**

Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych" przez firmy zewnętrzne na podstawie zawartych umów. W umowie musi znajdować się zapis o powierzeniu danych osobowych.

W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie

dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych.

Przeglądy techniczne wykonywane powinny być na bieżąco w miarę zgłaszania takich potrzeb przez użytkowników systemu osobie do tego upoważnionej.

Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, oraz nośników informacji służących do przetwarzania danych osobowych pełni administrator danych. Administrator danych prowadzi dokumentację potwierdzającą wykonanie napraw, przeglądów i konserwacji.

Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracownika Domu innego niż informatyk.

12. **Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych**

Administrator danych ma prawo i obowiązek dokonywania kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych.

Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

Załącznik Nr 2 do Instrukcji
Zarządzania Systemem Informatycznym
Służącym do przetwarzania danych
osobowych

Instrukcja postępowania z danymi z wizyjnego monitoringu

1/ Danymi z wizyjnego monitoringu domu, każdorazowo dysponuje administrator danych osobowych, zwany dalej ADO – w zakresie:
   a) ich udostępniania organowi nadzoru,
   b) ich udostępniania organom porządku publicznego,
   c) ich udostępniania pracownikom domu.

2/ ADO udostępnia dane z wizyjnego monitoringu domu w/w podmiotom w sytuacjach dotyczących bezpieczeństwa i porządku wewnętrznego w Domu.

3/ W systemie wizyjnego monitoringu domu stosuje się mechanizmy kontroli dostępu do danych w zakresie:
   a) rejestrowania każdego użytkownika indywidualnego,
   b) rejestrowania każdego użytkownika instytucjonalnego.

4/ System wizyjnego monitoringu domu zabezpiecza się w szczególności przed:
   a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu,
   b) utratą danych spowodowaną awarią zasilania, zakłóceniami w sieci zasilającej lub mechanicznymi uszkodzeniami systemu.

5/ Dane z wizyjnego monitoringu domu podlegają rejestracji zgodnie z następującymi zasadami:
   a) rejestracji danych dokonuje pracownik wyznaczony do obsługi informatycznej (ABI),
   b) rejestracji danych dokonuje się na nośniki informacji,
   c) nośniki informacji przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
   d) nośniki informacji rejestruje się w stosownej ewidencji,
   e) nośniki informacji kasuje się po ustaniu ich użyteczności.

6/ W przypadku wykrycia jakichkolwiek zagrożeń systemu wizyjnego monitoringu Domu a w szczególności: zniszczenia i uszkodzenia fizycznego, ingerencji osób nieuprawnionych wewnątrz lub z zewnątrz Domu, każdy użytkownik indywidualny niezwłocznie zawiadamia ADO.

Załącznik Nr 1 do Instrukcji
Zarządzania Systemem Informatycznym
Służącym do przetwarzania danych
osobowych

Instrukcja alarmowa dotycząca bezpieczeństwa informacyjnego

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1/. Każdy pracownik Domu w przypadku stwierdzenia zagrożenia lub naruszenie ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego , Administratora Bezpieczeństwa Informacji (ABI) lub ADO.

2/. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3/. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu , pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata /zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych, sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4/. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b) inicjuje ewentualne działania dyscyplinarne,
   c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
   d) dokumentuje prowadzone postępowania.

5/. W przypadku stwierdzenia incydentu (naruszenia), Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   b) zabezpiecza ewentualne dowody,
   c) ustala osoby odpowiedzialne za naruszenie,
   d) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   e) inicjuje działania dyscyplinarne,
   f) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   g) dokumentuje prowadzone postępowania.

Załącznik Nr 3 do Instrukcji
Zarządzania Systemem Informatycznym
Służącym do przetwarzania danych
osobowych

Instrukcja korzystania z kart Pekaobiznes

1/ Karty do podpisu przelewów w Pekaobiznes 24 przechowywane są w zamkniętej szafie metalowej w pomieszczeniu kasy Domu.

2/ Hasła do kart znane są tylko użytkownikom tj. właścicielom kart.

3/ Hasła do kart są poufne, niedopuszczalne jest ujawnienie haseł nieupoważnionym osobom.

4/ Główny księgowy na ustną prośbę użytkownika wydaje kartę do rąk własnych dla celów wynikających z obowiązków służbowych.

5/ Po wykonaniu przez użytkownika obowiązków służbowych związanych z użyciem karty zwraca on kartę do głównego księgowego.

6/ Niedopuszczalne jest wydanie karty osobie innej niż użytkownik.

7/ Użytkownik odpowiada za należyte wykorzystanie karty oraz za nieujawnianie haseł innym osobom.

8/ Główny księgowy odpowiada za należyte przechowywanie kart.

9/ Podczas nieobecności głównego księgowego w/w obowiązki przekazane są wyznaczonemu pracownikowi.

Załącznik nr 6 do *Zarządzenia* Nr 2 /2014
Dyrektora Domu Pomocy Społecznej
Im. W. Michelisowej w Lublinie
z dnia 6 marca.. 2014r.
w sprawie ochrony danych osobowych
w Domu Pomocy Społecznej
im. W. Michelisowej w Lublinie

OŚWIADCZENIE
PRACOWNIKA W SPRAWIE KORZYSTANIA Z SIECI KOMPUTEROWEJ
W Domu Pomocy Społecznej im. W. Michelisowej w Lublinie

Ja niżej podpisany / a własnoręcznym podpisem potwierdzam co następuje:

1/. Zostałem /am / poinformowany /a /, że urządzeni służące do łączności, takie jak telefony, Internet, fax, skrzynki e-mail, itp. Służą wyłącznie do załatwienia spraw służbowych.
W związku z tym, że Dyrekcja Domu Pomocy Społecznej In. W. Michelisowej w Lublinie w którym jestem zatrudniony /a/ , zastrzegła sobie prawo do dyscyplinarnego karania stwierdzonych przypadków wykorzystywania zakładowych urządzeń łączności do celów prywatnych, wyrażam zgodę na kontrolowanie mojej korespondencji, prowadzonej przy użyciu sprzętu biurowego / np. zawartość skrzynki e-mail, korzystanie z Internetu /

2/. Potwierdzam, że zostałem /am/ poinformowany / a/ w sposób nie budzący żadnych wątpliwości o zakazie instalowania dodatkowego oprogramowania w sieci komputerowej eksploatowanej przez Dom Pomocy Społecznej.

3/. Przyjmuję do akceptującej wiadomości fakt, że każda próba uruchomienia dodatkowego oprogramowania będzie traktowana przez Dom jako działanie na jego szkodę, a w przypadku jakichkolwiek kłopotów wynikających z nie przestrzegania przeze mnie w/w zaleceń, poniosę wszystkie wynikające z tego tytułu koszty, np. kary z tytułu użytkowania oprogramowania bez wymaganej licencji, uszkodzenie zakładowej sieci komputerowej , wprowadzenie do sieci komputerowej „ wirusów „ poprzez korzystanie z nielegalnych programów.

4/ Akceptuję zasadę, że wszystkich napraw sprzętu i oprogramowania, zarówno stanowiskowego jak i sieciowego oraz sprzętu telefonicznego, mogą dokonywać wyłącznie upoważnieni pracownicy.

.....
/czytelny podpis osoby składającej oświadczenie

.....
/ stanowisko /

Lublin dnia.....

Złożono do akt osobowych

.....