Zarządzenie Nr 6/2015
Dyrektora Domu Pomocy Społecznej
im. Wiktorii Michelisowej w Lublinie
z dnia 15 czerwca 2015 r.

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

Na podstawie art. 36 ust.1 i 36a ust. 1- 8 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182 z późn. zm.), §3 ust.1 rozporządzenia MSWiA 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. Nr 100 poz. 1024) oraz § 8 ust.7 regulaminu organizacyjnego Domu Pomocy Społecznej im. W. Michelisowej w Lublinie przyjętego zarządzeniem Nr 29/3/2013 Prezydenta Miasta Lublin z dnia 12 marca 2013r w sprawie przyjęcia regulaminu organizacyjnego Domu Pomocy Społecznej im. W. Michelisowej w Lublinie, zarządzam, co następuje:

§ 1

1. Wprowadzam Politykę Bezpieczeństwa w Domu Pomocy Społecznej im. Wiktorii Michelisowej w Lublinie stanowiącą Załącznik Nr 1 do zarządzenia.
2. Wprowadzam Instrukcję Zarządzania Systemem Informatycznym w Domu Pomocy Społecznej im Wiktorii Michelisowej w Lublinie stanowiącą Załącznik Nr 2 do zarządzenia.

§ 2

1. Nadzór nad przetwarzaniem danych osobowych w Domu Pomocy Społecznej im. W. Michelisowej sprawuje Administrator Bezpieczeństwa Informacji, zwany dalej ABI, wyznaczony przez dyrektora Domu – Administratora Danych Osobowych.
2. Zadaniem ABI jest zapewnienie przestrzegania przepisów o ochronie danych osobowych w jednostce oraz 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, prowadzenie rejestru zbioru danych osobowych prowadzonych przez jednostkę.
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.

§ 3

1. Zobowiązuję ABI do zgłoszenia swojej kandydatury do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych w terminie 30 dni od daty wejścia w życie niniejszego zarządzenia.
2. Wykonanie zarządzenia powierzam ABI, kierownikom komórek organizacyjnych Domu, inspektorowi ds. pracowniczych oraz innym pracownikom (osobom) upoważnionym do przetwarzania danych osobowych.
3. Nadzór nad realizacją zarządzenia powierzam ABI.
4. Dotychczasowe upoważnienia i oświadczenia pracowników złożone przed wejściem w życie zarządzenia tracą swoją aktualność.

§ 4

Zarządzenie obowiązuje od dnia 15 czerwca 2015 r.

§ 5

Traci moc zarządzenie Dyrektora Nr 2/2014 z dnia 06.03.2014 r. w sprawie: ochrony danych osobowych w Domu Pomocy Społecznej im. W. Michelisowej w Lublinie.

Załącznik Nr 1 - Polityka Bezpieczeństwa
Załącznik Nr 2 - Instrukcja Zarządzania Systemem Informatycznym

DYREKTOR
Domu Pomocy Społecznej
im. W. Michelisowej
w Lublinie
mgr Jolanta Ślązak-Chabros

Zał. Nr 1 do Zarządzenia Nr 6/2015
Dyrektora Domu Pomocy Społecznej
im Wiktorii Michelisowej w Lublinie
z dnia 15 czerwca 2015 r.
w sprawie ochrony danych osobowych
Domu Pomocy Społecznej
im Wiktorii Michelisowej w Lublinie

POLITYKA BEZPIECZEŃSTWA
w Domu Pomocy Społecznej im. Wiktorii Michelisowej w Lublinie

Część I – Wstęp

§ 1

Zgodnie z art. 36 ust.1 i 36a ust.1-8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych(t.j. Dz.U. z 2014 r. poz. 1182 z późn. zm.), zwanej dalej „ustawą" oraz 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), zwanego dalej „rozporządzeniem", ustanawia się „Politykę Bezpieczeństwa" w Domu Pomocy Społecznej im. W. Michelisowej w Lublinie.

§ 2

Ilekroć w niniejszym dokumencie jest mowa o jednostce organizacyjnej, należy przez to rozumieć Dom Pomocy Społecznej im. W. Michelisowej w Lublinie.

Część II – Zasady przetwarzania i ochrony danych osobowych

§ 3

Każda osoba, mająca dostęp do danych osobowych przetwarzanych w jednostce organizacyjnej jest zobowiązana do zapoznania się z niniejszym dokumentem.

§ 4

Wymagany przez rozporządzenie wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (zwany dalej „obszarem przetwarzania") stanowi załącznik nr 1 do niniejszego dokumentu.

§ 5

Wymagany przez rozporządzenie wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, stanowi załącznik nr 2 do niniejszego dokumentu.

§ 6

Osoby, które przetwarzają w jednostce organizacyjnej dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (załącznik nr 3 do niniejszego dokumentu) oraz podpisać oświadczenie o zachowaniu poufności tych danych (załącznik nr 4 do niniejszego dokumentu). Oświadczenie i upoważnienie o których mowa wyżej przechowywane są w aktach osobowych i za ich aktualność odpowiada inspektor ds. pracowniczych.

§ 7

Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych w formie elektronicznej posiada swój identyfikator oraz hasło, pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło, określone zostały w części 2 Instrukcji Zarządzania Systemem Informatycznym.

§ 8

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w § 6 (załącznik nr 3 do niniejszego dokumentu), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności (załącznik nr 4 do niniejszego dokumentu).

§ 9

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 31 ust.1 ustawy.

§ 10

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego.

§ 11

Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz.

W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się poprzez pocięcie w niszczarce.

§ 12

Zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Domu Pomocy Społecznej im. W. Michelisowej w Lublinie, stanowiącej Załącznik nr 2 do zarządzenia w sprawie ochrony danych osobowych Domu Pomocy Społecznej im. W. Michelisowej w Lublinie.

§ 13

Nadzór nad przetwarzaniem danych osobowych w jednostce organizacyjnej sprawuje Administrator Bezpieczeństwa Informacji (zwany dalej „ABI") wyznaczony przez Administratora Danych Osobowych. W przypadku niewyznaczenia ABI, funkcje mu przypisane pełni Administrator Danych Osobowych osobiście. Upoważnienie wyznaczające ABI stanowi załącznik nr 5 do niniejszego dokumentu. ABI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 do niniejszego dokumentu.

§ 14

ABI prowadzi wykaz zbiorów danych osobowych przetwarzanych w jednostce organizacyjnej (załącznik nr 2 do niniejszego dokumentu) oraz, kiedy jest to wymagane przez przepisy, zgłasza zbiory do rejestracji do GIODO. W ramach nadzoru nad przetwarzaniem danych, ABI sprawdza w szczególności cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia danych osobowych. Upoważnienie do przetwarzania danych osobowych (załącznik nr 3 do niniejszego dokumentu) nadaje Administrator Danych Osobowych. ABI jest zobowiązany do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w jednostce organizacyjnej.

§ 15

1. ABI prowadzi następujące wykazy:
   a) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiące obszar przetwarzania (załącznik nr 1 do niniejszego dokumentu)
   b) wykaz zbiorów danych osobowych (załącznik nr 2)
   c) wykaz podmiotów, którym powierzono dane osobowe do przetwarzania (załącznik nr 8 do niniejszego dokumentu)

2. Inspektor ds. pracowniczych prowadzi następujące wykazy:
   a) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych (załącznik nr 6 do niniejszego dokumentu)
   b) wykaz podmiotów i osób, którym udostępniono dane (załączniki nr 7 i nr 9 do niniejszego dokumentu)

§ 16

Osoby upoważnione do przetwarzania danych mają obowiązek:

a) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem,
b) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym,
c) zabezpieczać je przed zniszczeniem.

§ 17

W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator Danych Osobowych (lub osoba przez niego wyznaczona) jest obowiązany poinformować tę osobę o:

a) adresie swojej siedziby i pełnej nazwie,
b) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
c) prawie dostępu do treści swoich danych oraz ich poprawiania,
d) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Część III – Postanowienia końcowe

§ 18

Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 49-54a ustawy o ochronie danych osobowych.

§ 19

W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych oraz 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.

§ 20

Niniejszy dokument wchodzi w życie z dniem podanym w zarządzeniu Dyrektora jednostki.

Załączniki:
Załącznik nr 1 – Wykaz pomieszczeń w których przetwarzane są dane osobowe,
Załącznik nr 2 – Wykaz zbiorów danych osobowych,
Załącznik nr 3 – Upoważnienie do przetwarzania danych osobowych,
Załącznik nr 4 – Oświadczenie osoby mającej dostęp do danych osobowych,
Załącznik nr 5 - Upoważnienie dla administratora bezpieczeństwa informacji,
Załącznik nr 6 – Ewidencja osób upoważnionych do przetwarzania danych osobowych,
Załącznik nr 7 – Wykaz udostępnień danych osobowych innym podmiotom,
Załącznik nr 8 – Wykaz podmiotów którym powierzono przetwarzania danych osobowych,
Załącznik nr 9 – Wykaz udostępnień danych osobowych osobom których dotyczą.

DYREKTOR
Domu Pomocy Społecznej
im. W. Michelisowej
w Lublinie
mgr Jolanta Ślązak-Chabros

.....
Dyrektor – Administrator Danych Osobowych

WYKAZ POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

(wszystkie miejsca, pomieszczenia, pokoje, w których dokonuje się operacji na danych osobowych)

L.p.	Lokalizacja – adres	Precyzyjne określenie pomieszczenia	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1.				
2.				
3.				
4.				
5.				
6.				
7.				

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

L.p.	Nazwa zbioru danych osobowych	Cel przetwarzania	Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	Sposób przepływu danych pomiędzy poszczególnymi systemami
1.					
2.					
3.					
4.					

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana .....

   o numerze PESEL .....

   zatrudnioną/-ego na stanowisku .....

   w .....

do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
(należy określić zbiory zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa)

Lp.	Zbiór danych osobowych	Przetwarzanie metodą tradycyjną (w formie papierowej)	Przetwarzanie w systemie informatycznym
1	Akta osobowe mieszkańców – decyzje, wywiady środowiskowe		
2	Indywidualny plan wspierania mieszkańca domu		
3	Dane medyczne mieszkańców domu		
4	Dane osobowe pracowników		

2. Identyfikator/Login (w przypadku przetwarzania w systemie informatycznym) : .....

3. Okres trwania upoważnienia: .....

Wystawił: .....
(podpis Administratora Danych Osobowych zgodnie z § 12 Polityki Bezpieczeństwa)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Załącznik nr 4 do Polityki Bezpieczeństwa

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz ..... .

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014r. poz. 1182 z poźn.zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

.....

(data i podpis osoby oświadczającej)

.....
(miejscowość, data)

UPOWAŻNIENIE DLA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI (ABI)

Na podstawie art. 36a ust.1 ustawy z dnia 29 sierpnia 1997 r. (t. j. Dz. U. z 2014 r. poz. 1182 z późn. zm.) o ochronie danych osobowych, z dniem ..... wyznaczam Administratora Bezpieczeństwa Informacji i powierzam tę funkcję

Panu/Pani .....

posługującemu/-ej się numerem PESEL: .....

Do obowiązków Administratora Bezpieczeństwa Informacji należy: w szczególności:

1. Zapewnienie przestrzegania przepisów o ochronie danych osobowych w jednostce.
2. Wdrożenie i nadzór nad prawidłową realizacją Polityki Bezpieczeństwa obowiązującej w jednostce organizacyjnej wdrożenie i nadzór nad prawidłową realizacją Polityki Bezpieczeństwa obowiązującej w jednostce organizacyjnej.
3. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
4. Zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym lub zabraniem przez osobę nieuprawnioną.
5. Zabezpieczenie danych przed ich przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
6. Prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki techniczne służące ich zabezpieczeniu.
7. Nadawanie upoważnienia do przetwarzania danych osobowych.
8. Prowadzenie rejestru zbiorów danych osobowych przetwarzanych w jednostce.
9. Nadzorowanie prowadzenia i aktualizowania dokumentacji ochrony danych osobowych.

.....
podpis w imieniu Administratora Danych Osobowych

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Administratora Bezpieczeństwa Informacji w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ustawę o ochronie danych osobowych oraz rozporządzenie wykonawcze wydane na podstawie art. 39a do wyżej wymienionej ustawy.

.....
podpis Administratora Bezpieczeństwa Informacji (ABI)

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko/komórka organizacyjna	Zakres *(określenie, do jakich zbiorów dana osoba ma dostęp, zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa)*	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator/Login w danym systemie informatycznym
1.						
2.						
3.						
4.						
5.						
6.						
7.						

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

L.p.	Imię i Nazwisko/Nazwa zbioru *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	Data udostępnienia	Nazwa podmiotu, któremu udostępniono dane *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)*	Cel udostępnienia *(podstawa prawna/numer umowy)*	Zakres udostępnionych danych *(jakie dane zostały udostępnione)*	Rodzaj zbioru/zasobu i jego lokalizacja *(np. papierowy wydruk, dane w formie elektronicznej)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

WYKAZ PODMIOTÓW KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH

Lp.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia oraz numer umowy powierzenia	Zakres powierzonych danych *(jakie dane zostały powierzone)*	Określenie zbioru/zasobu
1.					
2.					
3.					
4.					
5.					
6.					
7.					

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH OSOBOM KTÓRYCH DOTYCZĄ

L.p.	Imię i nazwisko osoby, której dane są udostępniane	Data udostępnienia	Rodzaj zbioru/zasobu i jego lokalizacja *(np. papierowy wydruk danych zawartych w określonym zbiorze)*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Załącznik nr 2 do Zarządzenia Nr 6/2015
Dyrektora Domu Pomocy Społecznej
im. W. Michelisowej w Lublinie
z dnia 15 czerwca 2015 r.
w sprawie ochrony danych osobowych
Domu Pomocy Społecznej
im. W. Michelisowej w Lublinie

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014r. poz.1182 z późn. zm.) oraz z § 3 ust. 1 i 5 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), ustanawia się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Domu Pomocy Społecznej im. W. Michelisowej w Lublinie.

Ilekroć w niniejszym dokumencie jest mowa o:

a) ustawie – należy przez to rozumieć ustawę, o której mowa wyżej,
b) rozporządzeniu – należy przez to rozumieć rozporządzenie, o którym mowa wyżej,
c) jednostce organizacyjnej – należy przez to rozumieć Dom Pomocy Społecznej im. W. Michelisowej w Lublinie,
d) ADO – należy przez to rozumieć Administratora Danych Osobowych w rozumieniu ustawy – dyrektora Domu Pomocy Społecznej im. W. Michelisowej w Lublinie,
e) ABI – należy przez to rozumieć Administratora Bezpieczeństwa Informacji w rozumieniu ustawy,
f) ASI – należy przez to rozumieć Administratora Systemu Informatycznego,
g) Instrukcji – należy przez to rozumieć niniejszy dokument,
h) Polityce Bezpieczeństwa – należy przez to rozumieć przyjęty do stosowania w jednostce organizacyjnej dokument zatytułowany: „Polityka Bezpieczeństwa w Domu Pomocy Społecznej im. Wiktorii Michelisowej w Lublinie",
i) użytkowniku – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym w drodze upoważnienia,
j) systemie informatycznym – należy przez to rozumieć system informatyczny, w którym przetwarzane są dane osobowe w jednostce organizacyjnej.

ASI wyznaczany jest przez ABI lub ADO drogą pisemnego upoważnienia. W przypadku nie wyznaczenia ASI, jego funkcję pełni ABI lub osoba pełniąca funkcję ABI. Wzór upoważnienia ASI stanowi załącznik nr 3 do „Polityki Bezpieczeństwa". ASI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 do „Polityki Bezpieczeństwa".

ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu.

Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych

z sieci publicznej i systemu informatycznego. Obowiązkiem ASI jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

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 ADO. 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 3 do „Polityki Bezpieczeństwa".

Upoważnienia do przetwarzania danych osobowych rejestrowane są w rejestrze osób upoważnionych do przetwarzania danych osobowych (Załącznik nr 6 do „Polityki bezpieczeństwa")

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 ABI. 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".

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 ", 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 programistę Domu kart sprzętu elektronicznego Domu tj komputerów, drukarek, kserokopiarek, skanerów.

Karta sprzętu zawiera w szczególności n/w 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.

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" 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**

ADO 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.

Załączniki:
Załącznik nr 1 – Instrukcja alarmowa dotycząca bezpieczeństwa informacyjnego,
Załącznik nr 2 – Instrukcja postępowania z danymi z wizyjnego monitoringu,
Załącznik nr 3 – Instrukcja korzystania z kart Pekaobiznes.

DYREKTOR
Domu Pomocy Społecznej
im. W. Michelisowej
w Lublinie

.....mgr Iwona Ślązak-Chabros.....
Dyrektor – Administrator Danych Osobowych

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.

DYREKTOR
Domu Pomocy Społecznej
im. W. Michelisowej
w Lublinie
mgr Jolanta Ślązak-Chabros

.....
Dyrektor – Administrator Danych Osobowych

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.

DYREKTOR
Domu Pomocy Społecznej
im. W. Michelisowej
w Lublinie
mgr Jolanta Ślązak-Chabros

.....
Dyrektor – Administrator Danych Osobowych

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.

DYREKTOR
Domu Pomocy Społecznej
im. W. Michelisowej
w Lublinie
mgr Jolanta Stązak-Chabros

.....
Dyrektor – Administrator Danych Osobowych