Zarządzenie Nr 18/2014
Dyrektora Zespołu Ośrodków Wsparcia w Lublinie
z dnia 8 maja 2014 r.

w sprawie ochrony danych osobowych w Zespole Ośrodków Wsparcia w Lublinie

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024) oraz § 7 ust. 7 Regulaminu Organizacyjnego Zespołu Ośrodków Wsparcia w Lublinie stanowiącego załącznik do Zarządzenia Nr 34/5/2013 Prezydenta Miasta Lublin z dnia 13 maja 2013 r. w sprawie zatwierdzenia Regulaminu Organizacyjnego Zespołu Ośrodków Wsparcia w Lublinie zarządzam, co następuje:

§1

1. Wyznaczam Panią Emilią Śliwińską jako Administratora Bezpieczeństwa Informacji zwanego dalej ABI w Zespole Ośrodków Wsparcia w Lublinie, zwanym dalej „Zespołem".
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 Zespołu 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 upoważnienia.
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. kard
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 przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są wszystkie budynki wchodzące w skład Zespołu tj.:

a) budynek Centrum Usług Socjalnych przy ul. Lwowskiej 28,
b) budynek Dziennego Ośrodka Adaptacyjnego dla Dzieci i Młodzieży z Niepełnosprawnością Intelektualną przy ul. Poturzyńskiej 1,
c) pomieszczenia Centrum Dziennego Pobytu dla Seniorów Nr 2 przy ul. Maszynowej 2
d) pomieszczenia Centrum Dziennego Pobytu dla Seniorów Nr 3 przy ul. Niecałej 16,
e) budynek Centrum Dziennego Pobytu dla Seniorów Nr 4 przy ul. Pozytywistów 16,
f) pomieszczenia Klubu Seniora „Pogodna" przy ul. Pogodnej 19,
g) pomieszczenia Klubu Seniora „Owocowa" przy ul. Owocowej 6,
h) budynek Ośrodka Wsparcia dla Osób z Niepełnosprawnością „Benjamin" przy ul. Zbożowej 22A,
i) budynek Środowiskowego Domu Samopomocy przy ul. Nałkowskich 78

2. Pracownicy socjalni posiadający przenośny, przekazany im w użytkowanie sprzęt komputerowy przetwarzają dane osobowe uczestników Zespołu dodatkowo poza obszarami wymienionymi w ust. 1.
3. Wzór oświadczenia pracownika, o którym mowa w ust. 2 stanowi Zał. Nr 3 do zarządzenia.
4. 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 wylogowywanie z systemu,
4) upewnienie się, czy dane zostały zarejestrowane,
5) zakończenie pracy związanej z przetwarzaniem danych powinno odpowiadać wszystkim regułom bezpieczeństwa informacji.
5. Kopie informatyczne, wydruki wykonywane są w miarę potrzeb.
6. Nośniki danych oraz wydruki, nieprzeznaczone do udostępniania przechowywane są w specjalnie zamykanych szafkach, do których dostęp mają tylko osoby uprawnione.
7. Wszelkie awarie systemu oraz naruszenia bezpieczeństwa wymagają natychmiastowego powiadomienia ABI lub ADO.
8. Polityka bezpieczeństwa informacji w zakresie przetwarzania danych osobowych zawarta jest w Zał. Nr 4 do zarządzenia.
9. Instrukcję zarządzania systemem informatycznym stanowi Zał. Nr 5 do zarządzenia.

§4

1. Wykaz zbiorów danych osobowych stanowią:
1) Akta osobowe uczestników i pracowników;
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) Dokumentacja ZFŚS,
7) Dane gromadzone w systemie zamówień publicznych;
8) Rejestr osób dopuszczonych do przetwarzania danych osobowych;

9) Dokumentacja medyczna;
10) Składnica akt
2. W/w dane są przetwarzane w Zespole w systemie informatycznym, w komputerach ewidencjonowanych w spisie inwentarzowym jednostki.
3. Wprowadza się bezwzględny zakaz użytkowania programów zainstalowanych nielegalnie.

§5

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

§6

Traci moc zarządzenie Dyrektora Nr 23/2010 z dnia 1 września 2010 r. w sprawie ochrony danych osobowych w Zespole Ośrodków Wsparcia w Lublinie (z późn. zm.)

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Maria Pawela

Mirosława Łuksza
radca prawny

Załącznik Nr 1 - wzór upoważnienia do dostępu i przetwarzania danych osobowych
Załącznik Nr 2 - wzór oświadczenia pracownika
Załącznik Nr 3 – wzór oświadczenia pracownika przetwarzającego dane osobowe na przenośnym sprzęcie komputerowym
Załącznik Nr 4 - polityka bezpieczeństwa informacji w zakresie przetwarzania danych osobowych
Załącznik Nr 5 - instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Załącznik Nr 1 do Zarządzenia Nr 18/2014
Dyrektora z dnia 8 maja 2014.
w sprawie ochrony danych osobowych
w Zespole Ośrodków Wsparcia w Lublinie

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 Zespołu Ośrodków Wsparcia w Lublinie w zakresie
.....
.....

Upoważnienie ważne jest w okresie wykonywania pracy w Zespole Ośrodków Wsparcia 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 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.)

.....
/podpis Dyrektora/

Przyjąłem/Przyjęłam do wiadomości i stosowania

.....
/data i podpis pracownika/

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

Załącznik Nr 2 do Zarządzenia Nr 18/2014
Dyrektora z dnia 8 maja 2014.
w sprawie ochrony danych osobowych
w Zespole Ośrodków Wsparcia w Lublinie

.....
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 w tajemnicy danych osobowych, do przetwarzania których zostałem(am) upoważniony(a),
- nie ujawniania żadnych wiadomości z tym związanych,
- ochrony danych przed udostępnieniem osobom nieupoważnionym, 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 18/2014
Dyrektora z dnia 8 maja 2014.
w sprawie ochrony danych osobowych
w Zespole Ośrodków Wsparcia w Lublinie

.....
imię i nazwisko pracownika

.....
seria i nr dowodu osobistego

O Ś W I A D C Z E N I E

Oświadczam, iż zostałem/am przeszkolony/a i poinformowany/a o zagrożeniach oraz odpowiedzialności prawnej dotyczącej przetwarzania danych osobowych uczestników Zespołu, znajdujących się na przenośnym, przekazanym mi w użytkowanie sprzęcie komputerowym jednostki o numerze inwentarzowym ....., a w szczególności o:

1. Zachowaniu należytej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarami wymienionymi w § 3 ust. 1 Zarządzenia Wewnętrznego Nr 18/2014 Dyrektora Zespołu z dnia 8 maja 2014 r. w sprawie ochrony danych osobowych w Zespole Ośrodków Wsparcia w Lublinie,
2. Konieczności stosowania środków ochrony kryptograficznej wobec przetwarzanych danych,
3. Zakazie użytkowania przenośnego komputera w domu oraz instalowania i kopiowania jakichkolwiek aplikacji i programów bez zgody Dyrektora Zespołu.

Zostałem/am zapoznany/a z obowiązkami wynikającymi z następujących aktów prawnych:

1) Zarządzenie Wewnętrzne Nr 8/2014 Dyrektora Zespołu Ośrodków Wsparcia w Lublinie z dnia 8 maja 2014 r. w sprawie ochrony danych osobowych w Zespole Ośrodków Wsparcia w Lublinie,
2) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002, Nr 101, poz. 926, ze zm.)

Zostałem/am również poinformowany/a o zasadach odpowiedzialności za naruszenie powyższych przepisów.

Zobowiązuje się do wykonywania zadań zgodnie z przekazanymi informacjami i obowiązującymi przepisami.

.....
/data i podpis pracownika/

Załącznik Nr 4 do Zarządzenia Nr 18/2014
Dyrektora z dnia 8 maja 2014.
w sprawie ochrony danych osobowych
w Zespole Ośrodków Wsparcia w Lublinie

POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE OŚRODKÓW WSPARCIA 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 Zespole informacji zawierających dane osobowe.

§2

Określenia użyte w Polityce Bezpieczeństwa oznaczają:
1. Komórka organizacyjna - odpowiednio komórki organizacyjne, o których mowa w regulaminie organizacyjnym Zespołu;
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. System informatyczny - system przetwarzania danych w Zespole – wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
6. 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 Zespół 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 informatycznym Zespołu 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 Zespołu 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 Zespołu 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

§ 8

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

§9

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

§10

Administratorem danych osobowych Zespołu jest Dyrektor.

§11

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

§12

1. Obowiązki wynikające z ustawy o ochronie danych osobowych Dyrektor Zespołu powierza kierownikom komórek organizacyjnych Zespołu w zakresie podległych im pracowników oraz ABI.
2. Kierownicy komórek organizacyjnych Zespołu odpowiadają za realizację wymagań obowiązujących przepisów prawa, dotyczących ochrony danych osobowych, z obowiązkiem współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie swoich właściwości;
3. Z-cy dyrektora i kierownicy komórek organizacyjnych Zespołu zobowiązani są do zapoznania podległych pracowników z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), i zarządzeniem wewnętrznym Dyrektora w tym zakresie.

§13

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

VII. Przetwarzanie danych osobowych

§14

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

§15

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

§16

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

VIII. Archiwizowanie informacji zawierających dane osobowe

§17

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 Zespołu w sprawie instrukcji organizacji i zakresie działania składnicy akt.

DYREKTOR
Maria Pawela

Załącznik nr 5 do *Zarządzenia* Nr 18/2014
Dyrektora z dnia 8 maja 2014 r.
w sprawie ochrony danych osobowych
w Zespole Ośrodków Wsparcia 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 Zespołu. 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 inspektora ds. kadr.

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 Zespole 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 8 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.

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. 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.

5. 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.

6. Instrukcja alarmowa dotycząca bezpieczeństwa informatycznego.- zał. Nr 1

7. 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.

DYREKTOR

Maria Pawela

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 Zespołu w przypadku stwierdzenia zagrożenia lub naruszenia 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 komputerów, twardych dysków, oprogramowania, pomyłki 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
Maria Pawela