Załącznik Nr 1
do Zarządzenia Nr 18 / 2018
Dyrektora Domu Pomocy Społecznej
Piłka – Zamyślin
z dnia 22 maja 2018 roku

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH w DOMU POMOCY SPOŁECZNEJ PIŁKA - ZAMYŚLIN

POSTANOWIENIA OGÓLNE

§ 1

Celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Domu Pomocy Społecznej Piłka - Zamyślin, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania tych danych w Domu Pomocy Społecznej Piłka - Zamyślin.

§ 2

Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Domu Pomocy Społecznej Piłka - Zamyślin.

§ 3

Ilekroć w Polityce jest mowa o:

1) **Jednostce Organizacyjnej** - rozumie się przez to Dom Pomocy Społecznej Piłka - Zamyślin,
2) **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
3) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej),

4) **przetwarzaniu danych** - rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
5) **systemie informatycznym** - system przetwarzania danych w Domu Pomocy Społecznej Piłka - Zamyślin wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
6) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze,
7) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
8) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
9) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** - rozumie się przez to Dyrektora Domu Pomocy Społecznej Piłka - Zamyślin, który decyduje o celach i środkach przetwarzania danych osobowych,
10) **Inspektorze Ochrony Danych Osobowych (IODO)** - rozumie się przez to osobę wyznaczoną przez Dyrektora Domu Pomocy Społecznej Piłka - Zamyślin, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
11) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę wyznaczoną przez Dyrektora Domu upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym,
12) **zabezpieczenie systemu informatycznego** – rozumie się przez to wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą,
13) **kierowniku komórki organizacyjnej –** rozumie się przez to samodzielne stanowisko pracy,
14) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez Dyrektora Domu wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika,
15) **zgodzie osoby, której te dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa

oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Rozdział I
CELE

§ 4

Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.

§ 5

Dane osobowe w Domu Pomocy Społecznej Piłka - Zamyślin są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Domu na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 6

1. W systemie informacyjnym Domu przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
2. Politykę Bezpieczeństwa stosuje się do:
   a) danych osobowych mieszkańców Domu przetwarzanych w systemie informatycznym,
   b) wszystkich informacji dotyczących danych pracowników Domu, w tym danych osobowych personelu i treści zawieranych umów o pracę,
   c) wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
   d) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
   e) ewidencji osób upoważnionych do przetwarzania danych osobowych,
   f) innych dokumentów zawierających dane osobowe.
3. Zakresy określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do całego systemu informacyjnego Domu, w szczególności do:
   a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
   b) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,

c) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

4. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.
5. Każdy pracownik lub inna osoba mogąca mieć dostęp w systemie tradycyjnym lub informatycznym do informacji podlegających ochronie, podpisuje oświadczenie o zapoznaniu się z obowiązującą w Domu Polityką Bezpieczeństwa i zobowiązaniu do ochrony przetwarzanych w nim danych osobowych (Załącznik Nr 1). Oświadczenie przechowywane jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji IODO.
6. Każdy pracownik Domu (w tym stażysta, praktykant) zostaje poinformowany o celach, w jakich będą wykorzystywane jego dane osobowe, jednocześnie podpisuje zgodę na przetwarzanie swoich danych osobowych przez Dom (Załącznik Nr 2).
7. Kandydat na wolne stanowisko ma obowiązek umieścić w składanych osobiście w sekretariacie Domu lub wysyłanych e-mailowo dokumentach informację o zgodzie na przetwarzanie jego danych osobowych na potrzeby rekrutacji.
8. Dane osobowe kandydatów na wolne stanowiska w Domu będą przetwarzane jedynie do celów niezbędnych na potrzeby przeprowadzanej rekrutacji. Po jej zakończeniu zostaną niezwłocznie usunięte.
9. Osoby dostarczające dokumenty zawierające dane osobowe poza rekrutacją, mają obowiązek umieścić w składanych osobiście w sekretariacie Domu lub wysyłanych e-mailowo dokumentach informację o zgodzie na przetwarzanie jego danych osobowych. Dokumenty te będą przechowywane przez okres 6 miesięcy w kadrach i nie będą podlegały przetwarzaniu do momentu, gdy nie zajdzie potrzeba wykorzystania ich do celów rekrutacyjnych. Po upływie okresu przechowywania lub wykorzystania ich do celów rekrutacyjnych dokumenty ulegają niezwłocznemu zniszczeniu.
10. W przypadku gdy dokumenty w procesie rekrutacyjnym lub pozarekrutacyjnym będą pozbawione zgody na przetwarzanie danych osobowych kandydata, zostaną one niezwłocznie zniszczone, a taka osoba zostanie poproszona o ponowne dostarczenie dokumentów zawierających stosowne oświadczenie.

§ 7

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Domu zasad ochrony danych osobowych.
2. 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.

3. Dane osobowe mogą być udostępnione podmiotom upoważnionym do ich otrzymania na podstawie przepisów prawa, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
4. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 8

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

§ 9

Polityka Bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:
a) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego,
b) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

§ 10

Procedury i zasady określone w niniejszej Polityce Bezpieczeństwa stosuje się do wszystkich pracowników Domu Pomocy Społecznej Piłka - Zamyślin mających dostęp do danych osobowych przetwarzanych w Jednostce Organizacyjnej.

§ 11

1. Przetwarzanie danych osobowych do celów związanych z działalnością Jednostki Organizacyjnej jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.
2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.
3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.
4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Jednostki Organizacyjnej powinna być dokonywana indywidualnie w każdej sytuacji .

§ 12

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:
   a) adresie swojej siedziby i pełnej nazwie,
   b) celu zbierania 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.
2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 13

1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, należy poinformować osobę, której dane zostały zebrane, o:
   a) adresie swojej siedziby i pełnej nazwie,
   b) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
   c) źródle danych,
   d) prawie dostępu do treści swoich danych oraz ich poprawiania,
   e) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów Jednostki Organizacyjnej, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
   f) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów Jednostki Organizacyjnej, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy Jednostka Organizacyjna zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.
2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 14

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują kierownicy poszczególnych działów Jednostki Organizacyjnej.

§ 15

1. Pracownik musi zostać pisemnie upoważniony przez ADO do przetwarzania danych osobowych. W upoważnieniu należy wyszczególnić zbiory danych

osobowych, które będą poddawane przetwarzaniu przez pracownika (Załącznik Nr 3). Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy.
2. Upoważnienie przechowywane jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji IODO.
3. Ewidencję osób uprawnionych do przetwarzania danych osobowych prowadzi IODO (Załącznik Nr 4).

§ 16

1. Każdy nowo przyjęty mieszkaniec Domu zostaje poinformowany o celach, w jakich będą wykorzystywane jego dane osobowe, jednocześnie podpisuje zgodę na przetwarzanie swoich danych osobowych przez Dom (Załącznik Nr 5). W przypadku osób ubezwłasnowolnionych zgodę na przetwarzanie danych osobowych podpisuje jego opiekun prawny (Załącznik Nr 5A).
2. Podpisana zgoda na przetwarzanie danych osobowych mieszkańca znajduje się w jego aktach osobowych.

§ 17

1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w jednostce organizacyjnej dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.
2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi.

Rozdział II
ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 18

1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada:
   a) Administrator Danych,
   b) Inspektor Ochrony Danych Osobowych.
2. Kierownicy poszczególnych działów obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą uszkodzeniem lub zniszczeniem.

§ 19

Administrator Danych zobowiązany jest do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

a) określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
b) określenie pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
c) zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
d) wdrażanie i nadzorowanie przestrzegania Polityki Bezpieczeństwa,
e) stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
f) odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
g) określanie, które osoby i na jakich prawach mają dostęp do danych informacji.

§ 20

1. Administrator Danych Osobowych ma obowiązek powołać Inspektora Ochrony Danych Osobowych, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
2. IODO wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.
3. IODO jest zobowiązany poprzez zastosowanie odpowiednich środków i metod kontroli dostępu do zapewnienia wyłącznie uprawnionemu użytkownikowi dostępu do systemów informatycznych i tradycyjnych.
4. Inspektor Ochrony Danych Osobowych:
   a) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
   b) określa strategię zabezpieczania systemów informatycznych Domu,
   c) sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
   d) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Domu,
   e) określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
   f) sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach i pamięciach wymiennych oraz innych urządzeniach, w których są gromadzone i przetwarzane dane osobowe,
   g) sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,

h) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
i) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
j) zatwierdza wnioski o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
k) powiadamia Administratora Systemu Informatycznego o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
l) prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
m) prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
n) prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
o) prowadzi rejestr zbiorów danych osobowych Domu (przetwarzanych metodą tradycyjną lub w systemach informatycznych),
p) prowadzi rejestr czynności przetwarzania danych osobowych, dotyczący zarówno mieszkańców jak i pracowników Domu,
q) doradza użytkownikom w zakresie bezpieczeństwa,
r) dba, aby użytkownicy mający dostęp do systemu posiadali stosowne upoważnienia oraz byli przeszkoleni w zakresie obowiązujących regulacji bezpieczeństwa,
s) prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych.

§ 21

1. Administrator Danych Osobowych wyznacza Administratora Systemu Informatycznego, który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI lub w szczególnych przypadkach osoba wyznaczona przez niego jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.
2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany poprzez zastosowanie odpowiednich środków i metod kontroli dostępu do zapewnienia wyłącznie uprawnionemu użytkownikowi dostępu do systemów informatycznych.
3. Administrator Systemu Informatycznego odpowiedzialny jest za:
   a) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   b) optymalizację wydajności systemu informatycznego i baz danych,
   c) instalacje i konfiguracje sprzętu sieciowego i serwerowego,

d) instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
e) konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
f) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
g) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego,
h) zarządzanie kopiami awaryjnymi danych, w tym danych osobowych, oraz zasobów umożliwiających ich przetwarzanie,
i) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
j) przyznawanie na wniosek Administratora Danych, za zgodą Inspektora Ochrony Danych Osobowych, ściśle określonych praw dostępu do informacji w danym systemie,
k) wnioskowanie do Inspektora Ochrony Danych Osobowych w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
l) zarządzanie licencjami i procedurami ich dotyczącymi,
m) prowadzenie profilaktyki antywirusowej.

4. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem bezpieczeństwa przez Inspektora Ochrony Danych Osobowych.

§ 22

Kierownik danego działu odpowiada za przestrzeganie ustawy o ochronie danych osobowych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

a) kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników,
b) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie,
c) zgłasza IODO planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie,
d) wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom,
e) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Domu Pomocy Społecznej Piłka - Zamyślin.

§ 23

Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed IODO za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

§ 24

1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.
4. Urządzenia, dyski lub inne informatyczne nośniki danych przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora.

§ 25

W Domu rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   a) pomieszczenia zamykane na klucz,
   b) szafy pancerne z zamkami.
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   a) przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   b) przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:
   a) osobą odpowiedzialną za bezpieczeństwo danych jest Administrator Danych oraz Inspektor Ochrony Danych Osobowych,
   b) Inspektor Ochrony Danych Osobowych na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami.

Rozdział III
WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

§ 26

1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci

dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).
2. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi Załącznik Nr 6.
3. W Domu prowadzone są rejestry czynności przetwarzania danych osobowych mieszkańców Domu (Załącznik Nr 7) oraz pracowników Domu (Załącznik Nr 8).
4. Dom prowadzi zbiór zagrożeń możliwych do wystąpienia podczas przetwarzania danych osobowych (Załącznik Nr 9).

§ 27

Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Domu Pomocy Społecznej Piłka - Zamyślin wyróżnia się dwie kategorie danych:
1) **dane osobowe zwykłe** - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych.
2) **dane osobowe szczególnie chronione** – wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 28

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:
a) stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 29

Każdy pracownik Domu, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym lub przetwarzanych w inny sposób, zobowiązany jest do niezwłocznego poinformowania o tym Inspektora Ochrony Danych Osobowych, który kontaktuje się w tej sprawie z ASI.

§ 30

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

2. W stosunku do danych, które zostały zagubione lub pozostawione bez nadzoru poza obszarem bezpieczeństwa, należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§ 31

1. Gdy ASI stwierdzi lub uzyska informację wskazującą na naruszenie ochrony tej bazy danych, zobowiązany jest do niezwłocznego:
   a) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
   b) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
   c) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,
   d) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in. szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
   e) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną tą samą drogą.
2. W przypadku naruszenia ochrony danych osobowych, Administrator Danych bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych. Wzór wniosku stanowi Załącznik Nr 10.
3. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
4. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
5. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
6. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu, należy wyciągnąć konsekwencje dyscyplinarne.

Rozdział IV
SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 32

1. Ustala się następującą organizację pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
   a) w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
   b) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone oraz czy zabezpieczenia te nie były naruszone,
   c) w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu bądź zmiany przez osoby do tego celu nieupoważnione,
   d) po zakończeniu przetwarzania danych, pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.
2. Obieg dokumentów zawierających dane osobowe pomiędzy komórkami organizacyjnymi jednostki, winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).
3. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji Jednostka Organizacyjna - mieszkańcy, przedsiębiorcy, kontrahenci, Zakład Ubezpieczeń Społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski i inne jednostki administracji samorządowej i rządowej.
4. Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Domu i sieci zewnętrznych (typu Plus, Era, Orange, Play, pozostałe sieci komórkowe, WiFi , WiMAX itp.).

Rozdział V
OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 33

1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administrator Systemu Informatycznego zapewniający jego prawidłową eksploatację.
2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.
3. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, by uniemożliwić tym osobom wgląd w dane osobowe.
4. Dokumenty i nośniki informacji zawierające dane osobowe, powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu meblach biurowych posiadających odpowiednie zabezpieczenia.

Rozdział VI
UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 34

1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany w terminie 30 dni poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:
   a) jakie dane osobowe zawiera zbiór,
   b) w jaki sposób zebrano dane,
   c) w jakim celu i zakresie dane są przetwarzane,
   d) w jakim zakresie oraz komu dane zostały udostępnione.
2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1 udziela się na piśmie.

§ 35

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
   a) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
   b) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
   c) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
   d) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,

e) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
f) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane,
g) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów Administratora Danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
h) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów Administratora Danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy Administrator Danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 lit. a-e nie częściej niż raz na 6 miesięcy.

§ 36

1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych jest obowiązany bez zbędnej zwłoki do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.
2. Każda z osób zatrudnionych przy przetwarzaniu danych ma obowiązek poinformować IODO o wystąpieniu osoby, której dane dotyczą, o ich uaktualnienie, sprostowanie, czasowe lub stałe wstrzymanie przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

§ 37

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest Dyrektor Domu Pomocy Społecznej Piłka – Zamyślin lub pracownik posiadający wymagane prawem upoważnienie.

2. W przypadku udostępniania danych osobowych w celach innych niż wyłączenie do zbioru, Administrator Danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 38

Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO z uwzględnieniem wymagań określonych w ustawie o ochronie danych osobowych (Załącznik Nr 11).

Rozdział VII
ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 39

Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego, by nie spowodować jego uszkodzenia.

§ 40

1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.
2. Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł.

   W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

Rozdział VIII
BEZPIECZEŃSTWO FIZYCZNE

§ 41

1. Dane osobowe, które są przedmiotem przetwarzania zgodnie z przepisami ustawy o ochronie danych osobowych, gromadzone i przechowywane są w serwerze i w postaci tradycyjnej .
2. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 42

1. Obszar systemów informatycznych w Domu Pomocy Społecznej Piłka - Zamyślin obejmuje w oddziale Piłka i oddziale Zamyślin :
   a) wszystkie pomieszczenia biurowe,
   b) sale terapii zajęciowej,
   c) sale rehabilitacji,
   d) gabinety medyczne „KRYS-MED”,
   e) pomieszczenia socjalne.

2. IODO prowadzi ewidencję pomieszczeń stanowiących obszar przetwarzania danych osobowych w Domu Pomocy Społecznej Piłka – Zamyślin (Załącznik Nr 12).

§ 43

1. Pomieszczenia, w których znajdują się systemy informacji winny być:
   a) wyposażone w szafy lub meble biurowe zamykane na klucz, umożliwiające przechowywanie dokumentów,
   b) zamknięte, jeśli nikt w nich nie przebywa.
2. Każde z pomieszczeń jest zamykane na klucz.
3. Gabinety medyczne i pomieszczenia socjalne zabezpieczone są kluczami. Komplet kluczy upoważniony personel (pielęgniarki, opiekunowie) zdaje na koniec dyżuru pracownikom dyżur podejmującym. Personel kończący dyżur ma obowiązek odnotować w raporcie opiekunów o fakcie zdania kompletu kluczy.
4. Pomieszczenia terapii zajęciowej oraz gabinetu rehabilitacyjnego zabezpieczone są kluczem. W przypadku wystąpienia sytuacji, gdy pracownik musi opuścić pomieszczenie a znajdują się w nim mieszkańcy biorący udział w zajęciach z terapii zajęciowej lub rehabilitacji, pracownik ma obowiązek dopilnować, aby dane osobowe, które przetwarza w swoim pomieszczeniu, były odpowiednio zabezpieczone przed nieupoważnionym dostępem (szafy z dokumentami zakluczone, komputer wyłączony lub z wylogowanym kontem użytkownika).
5. Każdy z pracowników pracujących w danym pomieszczeniu odpowiedzialny jest za jego odpowiednie zabezpieczenie na czas nieobecności.

§ 44

Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą Administratora Danych Osobowych i pod kontrolą IODO, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

Rozdział IX
BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

§ 45

Sprzęt i oprogramowanie, indywidualnie lub łącznie, mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

§ 46

Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy ASI i IODO.

§ 47

Zabrania się instalowania i korzystania z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.

§ 48

1. Dostęp do zbiorów danych osobowych znajdujących się na serwerach następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.
2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.
3. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane zgłasza ten fakt IODO, który kontaktuje się z ASI w sprawie zmiany hasła i sprawdza, czy nie doszło do naruszenia tej bazy danych.

§ 49

1. Elektroniczne bazy danych osobowych są archiwizowane.
2. Kopie są wykonywane na oddzielnym nośniku elektronicznym (płyta CD).

§ 50

Używanie oprogramowania prywatnego w sieci Domu jest zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

Rozdział X
KONSERWACJE I NAPRAWY

§ 51

Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez ASI lub inne uprawnione osoby.

§ 52

1. Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.
2. Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest kierownik danego działu. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Systemu Informatycznego.

§ 53

Administrator Systemu Informatycznego przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

a) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w pomieszczeniu biurowym znajdującym się w strefie o ograniczonym dostępie,
b) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

Rozdział XI
PLANY AWARYJNE I ZAPOBIEGAWCZE

§ 54

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

§ 55

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na dwa tygodnie. Kopie archiwalne danych są wykonywane na nośnikach informatycznych, i przechowywane są przez Administratora Systemu Informatycznego. Użycie kopii zapasowych następuje na polecenie Administratora Systemu Informatycznego w przypadku odtwarzania systemu po awarii.

Rozdział XII
POLITYKA ANTYWIRUSOWA

§ 56

1. Wszystkie serwery i komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.
2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:
   a) nie należy używać innego oprogramowania na stacji roboczej innego niż zalecane przez Administratora Systemu Informatycznego,
   b) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.
3. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z ASI.

Rozdział XIII
PRZEPISY KOŃCOWE

§ 57

Naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

§ 58

W sprawach nie uregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy ustawy o ochronie danych osobowych, Rozporządzenia RODO 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 (Dz. U. z 2004 r. Nr 100, poz. 1024).