ZASADY POLITYKI BEZPIECZEŃSTWA

Danych osobowych

Wersja nr 5

§ 1

Podstawa prawna

1. Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych (tj. Dz. U. 2002 r. nr 101 poz. 926 z późn. zm.).
2. Rozporządzenie 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 systemu służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz 1024 z późn. zm.).
3. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. w sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej (Dz. U. Nr 216, poz 1609 z późn. zm.).

§ 2

Postanowienia ogólne i definicje

1) Celem przygotowania i wdrożenia niniejszego dokumentu jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych przez Ośrodek Pomocy Społecznej oraz podległą mu Noclegownię w Jastrzębiu-Zdroju.

2) Bezpieczeństwo danych osobowych rozumiane jest jako stan, w którym niemożliwe jest udostępnienie danych osobowych osobom nieupoważnionym, zabranie tych danych przez osoby nieupoważnione, przetwarzanie tych danych z naruszeniem prawa, zmiana, utrata, uszkodzenie lub zniszczenie, a także dokonywanie innych sprzecznych z prawem operacji na danych.

3) Ilekroć w Zasadach Polityki jest mowa o:

   a) **Administratorze Danych Osobowych (ADO)** – rozumie się przez to Dyrektora Ośrodka Pomocy Społecznej w Jastrzębiu-Zdroju,
   b) **Administratorze Bezpieczeństwa Informacji (ABI)** – rozumie się przez to osobę odpowiedzialną za bezpieczeństwo danych w systemie informatycznym, upoważnioną do pełnienia funkcji administratora przez Dyrektora Ośrodka Pomocy Społecznej,
   c) **Administratorze Systemu Informatycznego (ASI)** – oznacza osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej, upoważnioną do administrowania systemem przez Dyrektora Ośrodka Pomocy Społecznej,
   d) **SEPI** – rozumie się przez to Samorządową Elektroniczną Platformę Informacyjną,
   e) **OPS** - rozumie się przez to Ośrodek Pomocy Społecznej w Jastrzębiu-Zdroju, ul. Opolska 9,
   f) **PUP** – rozumie się przez to Powiatowy Urząd Pracy w Jastrzębiu-Zdroju, ul. Pszczyńska 134,
   g) **PEFS 2007** – rozumie się przez to Podsystem monitorowania Europejskiego Funduszu Społecznego,
   h) **Dyrektorze** – rozumie się przez to Dyrektora Ośrodka Pomocy Społecznej w Jastrzębiu-Zdroju,
   i) **Instrukcji** – rozumie się przez to Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych obowiązującą w Ośrodku Pomocy Społecznej,
   j) **Pracowniku** – rozumie się przez to pracownika Ośrodka Pomocy Społecznej zatrudnionego przy przetwarzaniu danych osobowych,
   k) **Zbiorze danych** – 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,

l) **Przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

m) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

n) **Użytkowniku** – oznacza to osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

o) **Przetwarzającym** – oznacza to podmiot, któremu powierzono przetwarzanie danych osobowych na podstawie umowy, o której mowa w art. 31 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych,

p) **Identyfikatorze Użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

q) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

r) **Uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

s) **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

t) **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

u) **Osobie upoważnionej** - osoba posiadająca upoważnienie wydane przez administratora danych osobowych (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu (listę osób upoważnionych do przetwarzania danych osobowych posiada administrator bezpieczeństwa informacji),

v) **Osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowanie i jego konserwację** – rozumie się przez to informatyka odpowiedzialnego za powyższe zadania wyznaczone przez Dyrektora, zwanego dalej „Informatykiem",

w) **Pomieszczeniach** – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych Osobowych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach,

x) **Danych osobowych** – oznacza to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne lub społeczne,

y) **Odbiorcy danych** – oznacza to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

i) osoby, której dane dotyczą,

ii) osoby, upoważnionej do przetwarzania danych osobowych.

z) **Ustawa** – oznacza Ustawę z dnia 29 sierpnia 1997 o ochronie danych osobowych (tj. Dz. U. 2002 r. nr 101 poz. 926 z późn. zm.),

aa) **Rozporządzenie** – oznacza Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. w sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej (Dz. U. Nr 216, poz 1609 z późn. zm.).

§ 3

Zakres obowiązków.

1) Administrator Danych Osobowych reprezentowany przez Dyrektora Ośrodka Pomocy Społecznej w szczególności:
   a) wyznacza osobę, która ma pełnić obowiązki Administratora Bezpieczeństwa Informacji,
   b) wydaje upoważnienia do przetwarzania danych osobowych,
   c) decyduje o celach i środkach przetwarzania danych osobowych.

2) Administrator Bezpieczeństwa Informacji w szczególności:
   a) nadzoruje przestrzeganie zasad ochrony danych osobowych,
   b) przygotowuje zgłoszenia rejestracyjne oraz aktualizacyjne zbiorów danych osobowych,
   c) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
   d) prowadzi wykaz pomieszczeń, w których przetwarzane są dane osobowe,
   e) przygotowuje i aktualizuje politykę bezpieczeństwa danych osobowych oraz instrukcje zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   f) interweniuje w sytuacji naruszenia systemu zabezpieczeń danych osobowych.

3) Administrator Systemu Informatycznego
   a) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe,

b) rejestruje i przydziela użytkownikom uprawnienia dostępu do systemu informatycznego na zasadach określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

c) odbiera użytkownikom uprawnienia dostępu do systemu informatycznego na polecenie Administratora Bezpieczeństwa Informacji,

d) zapobiega ujawnieniu danych osobowych zapisanych na informatycznych nośnikach danych,

e) interweniuje w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego,

f) rejestruje przypadki naruszeń zabezpieczeń systemu informatycznego,

g) kieruje wykonaniem napraw i konserwacją urządzeń należących do systemu informatycznego służącego do przetwarzania danych osobowych,

h) zarządza oraz nadzoruje likwidację nośników informatycznych, na których zapisane są dane osobowe,

i) administruje wykonywanie kopii zapasowych i ich przechowywanie,

j) odpowiada za utrzymanie w należytym stanie urządzeń zapewniających nieprzerwaną pracę (w tym brak zakłóceń zasilania komputerów i innych urządzeń należących do systemu informatycznego, w którym przetwarzane są dane osobowe).

§4

Powierzenie przetwarzania danych osobowych.

1. Zlecenie wykonania jakiejkolwiek czynności przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie na podstawie umowy zawartej na piśmie, której przykładowy wzór stanowi załącznik nr 4 do niniejszej Polityki.
2. Projekt umowy wymaga przed podpisaniem zatwierdzenia przez Administratora Bezpieczeństwa Informacji.

§ 5

Rejestracja zbiorów danych osobowych

1. Administrator Danych Osobowych prowadzi zbiory danych osobowych określone w §11 niniejszej polityki .
2. Za przygotowanie zgłoszeń rejestracyjnych oraz aktualizacyjnych zbiorów danych osobowych odpowiada Administrator Bezpieczeństwa Informacji.

3. Zgłoszeń dokonuje Administrator Danych Osobowych, reprezentowany przez Dyrektora Ośrodka Pomocy Społecznej.

§6

W przypadku zbierania danych nie od osoby, której one dotyczą, dokonujący tej czynności zobowiązany jest do poinformowania osoby, której dane dotyczą o:

1. adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2. celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3. źródle danych,
4. prawie dostępu do treści swoich danych oraz ich poprawiania,
5. o uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

Ww. obowiązek nie dotyczy przypadków określonych w art. 25 ust. 2 Ustawy.

§7

Udostępnienie danych osobowych

1. Dane osobowe udostępniane są na pisemny, umotywowany wniosek, chyba, że przepisy Ustawy stanowią inaczej. Wzór wniosku stanowi załącznik nr 10.
2. Osoba rozpatrująca wniosek, o którym mowa w ust. 1, w przypadku powzięcia jakichkolwiek wątpliwości co do dopuszczalności udostępnienia danych osobowych, przekazuje go ABI w celu rozpatrzenia.
3. W przypadku gdy podmiot występujący o udostępnienie danych osobowych, nie składający pisemnego wniosku, powołuje się na istniejące przepisy uprawniające go do otrzymania danych osobowych, osoba zatrudniona przez Administrator Danych Osobowych, do której zwrócono się o udostępnienie takich danych, pyta wnioskodawcę o podanie podstawy prawnej udostępnienia.
4. W przypadku powzięcia jakichkolwiek wątpliwości, co do dopuszczalności danych osobowych, w przypadku określonym w ust. 3, osoba, do której zwrócono się o udostępnienie danych osobowych zwraca się do Administratora Bezpieczeństwa Informacji o rozpatrzenie sprawy.

§8

Realizacja praw osób, których dane dotyczą.

1) Na wniosek osoby, której dane dotyczą, Administrator Danych Osobowych jest zobowiązany w terminie 30 dni poinformować o przysługujących jej prawach oraz udzielić, odnośnie jej danych osobowych, informacji, o których mowa art. 32 ust. 1 pkt. 1-5a Ustawy, a w szczególności podać w formie zrozumiałej:
   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) Osoba rozpatrująca wniosek, o którym mowa w ust 1, w przypadku powzięcia jakichkolwiek wątpliwości co do istnienia uprawnienia wnioskodawcy do otrzymania informacji objętych wnioskiem, przekazuje go Administratorowi Bezpieczeństwa Informacji w celu rozpatrzenia.
3) Na wniosek osoby, której dane dotyczą informacji o których mowa w ust 1, udziela się na piśmie.

§9

Współpraca z innymi podmiotami, udostępnianie danych ze zbioru danych zarejestrowanego w GIODO pod nazwą *DANE OSOBOWE KLIENTÓW OPS* jednostkom nadrzędnym oraz przetwarzanie obcych zbiorów danych osobowych, których administratorem nie jest OPS.

1. SEPI pozwala zacieśniać współpracę między jednostkami samorządowymi i lepiej realizować obowiązki zawarte w Ustawie z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz.U. 2004 nr 99 poz. 1001 z późn. zm.). W celu realizacji zadań została podpisana *UMOWA TRÓJSTRONNA nr It.1333.008.2014,* która jest załącznikiem nr 13 w sprawie udostępniania i wykorzystywania udostępnionych danych osobowych. Na mocy tej umowy OPS udostępnia Powiatowemu Urzędowi Pracy w Jastrzębiu-Zdroju, ul. Pszczyńska 134 do odczytu część danych zgromadzonych w zbiorze zarejestrowanym w GIODO pod nazwą *DANE OSOBOWE KLIENTÓW OPS*. PUP udostępnia OPS część danych zgromadzonych w zbiorze zarejestrowanym w GIODO pod nazwą *EWIDENCJA BEZROBOTNYCH I KLIENTÓW POWIATOWEGO URZĘDU PRACY W JASTRZĘBIU ZDROJU.* Umowa wraz z załącznikami jej dotyczącymi (m.in. upoważnienia do przetwarzania danych osobowych) znajduje się w załączniku nr 13 do Polityki Bezpieczeństwa Informacji. Załącznik nr 6 do w/w umowy stanowi osobną umowę dotyczącą przetwarzania

danych osobowych przez firmę Sygnity S.A. i jest on załącznikiem nr 14 do Polityki Bezpieczeństwa.

2. PEFS 2007 jest prowadzony na podstawie podpisanej umowy, która jest załącznikiem nr 15 oraz aktualnego aneksu, który jest załącznikiem nr 16 Podstawowym celem podsystemu jest spełnienie wszystkich wymogów Komisji Europejskiej, których ze względu na specyfikę EFS nie uwzględniono w Krajowym Systemie Informatycznym. PEFS 2007 został stworzony w celu ułatwienia realizacji projektów, wsparcia systemu ewaluacji, monitoringu, kontroli i sprawozdawczości w ramach PO KL. Administratorem danych osobowych tego zbioru jest instytucja zarządzająca PO KL. Załącznik nr 5 stanowi przykładowy wzór rejestru osób upoważnionych do przetwarzania danych osobowych w PEFS 2007, załącznik nr 7 stanowi wzór upoważnienia do przetwarzania danych osobowych w zbiorze PEFS 2007, załącznik nr 8 – wzór odwołania upoważnienia przetwarzania danych osobowych w zbiorze PEFS 2007, załącznik nr 17 to ewidencja pracowników upoważnionych do przetwarzania danych osobowych w związku z wykonywaniem umowy ramowej w ramach Programu Operacyjnego Kapitał Ludzki, załącznik nr 18 jest to opis struktury zbioru. Kompletna dokumentacja dotycząca tego zbioru znajduje się w Zespole Projektowym OPS, który ją prowadzi.
3. W OPS zostało uruchomione zasilanie Centralnego Systemu Informatycznego Zabezpieczenia Społecznego (CSIZS) w ramach systemu Emp@tia. Zasilanie jest wykonywane ze zbioru danych osobowych zarejestrowanego w GIODO pod nazwą *DANE OSOBOWE KLIENTÓW OPS*. Dane te są udostępniane na podstawie art. 23 ust. 4a Ustawy oraz §3 ust. 3 Rozporządzenia. Na tej samej podstawie oraz z tego samego zbioru przekazywany jest Zbiór Centralny do Śląskiego Urzędu Wojewódzkiego. Dane do zasilenia CSIZS są generowane i przekazywane za pomocą systemu Pomost Std, który na podstawie §12 ust. 6 Rozporządzenia ma świadectwo zgodności o nr 1/1.04/PS/GP/2015 (załącznik nr 24) wydane przez Ministra Pracy i Polityki Społecznej. Zbiory Centralne są generowane za pomocą tego samego systemu, a przekazywane przez Centralną Aplikację Statystyczną (CAS)

§10

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (Obszar) znajduje się w załączniku nr 1 do Zasad Polityki Bezpieczeństwa.

§ 11

Wykaz osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym prowadzi ASI.

1) Rejestr zawiera informacje o:
   a) Imieniu i nazwisku osoby upoważnionej,
   b) Dacie nadania i ustania oraz zakresie upoważnienia do przetwarzania danych,
   c) Identyfikatorze użytkownika, jeżeli dane przetwarzane są w systemie informatycznym.

§ 12

Wykaz zbiorów danych osobowych, których administratorem jest OPS wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

1) Ośrodek Pomocy Społecznej w Jastrzębiu-Zdroju przetwarza dane osobowe wyłącznie w zakresie niezbędnym do realizacji celów związanych z działalnością zgodnie z Ustawą z dnia 12 marca 2004 r. o pomocy społecznej (tj. Dz. U. z 2013 r. poz. 182 z późn. zm.), Ustawą o wspieraniu rodziny i systemie pieczy zastępczej z dnia 9 czerwca 2011 roku (tj. Dz.U. 2011 nr 149 poz. 887 z późn. zm.), Ustawą o przeciwdziałaniu przemocy w rodzinie (tj. Dz.U. 2005 nr 180 poz. 1493 z późn. zm.) i dbać będzie o to aby dane przetwarzane były zgodnie z prawem, zbierane dla oznaczonych zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Ośrodek Pomocy Społecznej podejmować będzie wszelkie wymagane przez przepisy prawa działania w celu ochrony danych przed dostępem do nich osób nieuprawnionych w sposób przewidziany w przepisach prawa.

2) W Ośrodku Pomocy Społecznej są następujące zbiory danych osobowych:
   a) **„DANE OSOBOWE KLIENTÓW OPS"** – do przetwarzania danych w tym zbiorze stosowany jest program Pomost STD, producent Sygnity S.A., Al. Jerozolimskie 180, 02-486 Warszawa, program Finanse, producent Rekord SI sp. z o. o., ul. Kasprowicza 5, 43-300 Bielsko-Biała, program Płatnik, producent Asseco Poland S.A., ul. Olchowa 14, 35-322 Rzeszów, dystrybutor Zakład Ubezpieczeń Społecznych, ul. Szamocka 3, 5, 01-748 Warszawa, programy Microsoft Office Word, Microsoft Office Excel, producent Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399,

USA, LibreOffice Writer, LibreOffice Calc producent The Document Foundation Kurfürstendamm 188, 10707 Berlin, Niemcy, stosowana jest również forma papierowa,

b) **„Przeciwdziałanie przemocy w rodzinie"** – do przetwarzania danych w tym zbiorze stosowane są programy Microsoft Office Word, Microsoft Office Excel, producent Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399, USA, LibreOffice Writer, LibreOffice Calc producent The Document Foundation Kurfürstendamm 188, 10707 Berlin, Niemcy, program Pomost STD, producent Sygnity S.A., Al. Jerozolimskie 180, 02-486 Warszawa, stosowana jest również forma papierowa,

c) **„EZD SIDAS"** – do przetwarzania danych w tym zbiorze stosowany jest program EZD SIDAS, producent Madkom S.A., Al. Zwycięstwa 96/98, 81-451 Gdynia,

d) **„Piecza zastępcza"** – do przetwarzania danych w tym zbiorze stosowany jest program Pomost STD, producent Sygnity S.A., Al. Jerozolimskie 180, 02-486 Warszawa, stosowana jest również forma papierowa,

e) **„REALIZACJA PROGRAMU AKTYWNY SAMORZĄD"** – do przetwarzania danych w tym zbiorze stosowane są programy Microsoft Office Word, Microsoft Office Excel, producent Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399, USA, LibreOffice Writer, LibreOffice Calc producent The Document Foundation Kurfürstendamm 188, 10707 Berlin, Niemcy, stosowana jest również forma papierowa,

f) **„DARMOWY INTERNET"** – do przetwarzania danych w tym zbiorze stosowana jest wyłącznie forma papierowa.

§ 13

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

1. **„DANE OSOBOWE KLIENTÓW OPS"** – dane przechowywane są w bazach danych Firebird, w bazie danych MS SQL, plikach programów Microsoft Office Word (*.doc, *.docx), Microsoft Office Excel (*.xls, *.xlsx), LibreOffice Writer (*.odt), LibreOffice Calc (*.ods) oraz w formie papierowej ,
2. **„Przeciwdziałanie przemocy w rodzinie"** – dane przechowywane są w bazie danych Firebird, plikach programów Microsoft Office Word (*.doc, *.docx), Microsoft Office Excel (*.xls, *.xlsx), LibreOffice Writer (*.odt), LibreOffice Calc (*.ods) oraz w formie papierowej,
3. **„EZD SIDAS"** – dane przechowywane są w bazie danych PostgreSQL oraz w formie papierowej,
4. **„Piecza zastępcza"** – dane przechowywane są w bazie danych Firebird oraz w formie papierowej,

5. **„REALIZACJA PROGRAMU AKTYWNY SAMORZĄD"** – dane przechowywane są w plikach typu *.docx, *.doc, *.odt, *.xlsx, *.xls oraz w formie papierowej,
6. **„DARMOWY INTERNET"** – dane przechowywane są wyłącznie w formie papierowej.

Struktury baz danych poszczególnych programów użytych do przetwarzania danych osobowych w OPS są określane przez producentów poszczególnych programów i są one dołączone w załącznikach. Zmiana struktury poszczególnej bazy danych nie wymaga zmiany Polityki Bezpieczeństwa w formie zarządzenia, a jest dokonywana przez ABI poprzez wydrukowanie i dołączenie aktualnej struktury bazy danych. Wersja Polityki Bezpieczeństwa nie zmienia się.

§ 14

Struktury danych oraz sposób przepływu informacji w poszczególnych programach do przetwarzania danych osobowych w OPS.

1) SEPI
   a) zestawienie struktur dokumentów elektronicznych w formacie XML, wraz z formatami danych oraz protokołami komunikacyjnymi i szyfrującymi oraz ogólny opis systemu znajduje się w załącznikach nr 25 i 26
2) PEFS
   a) Opis systemu PEFS 2007, sposób wypełniania go oraz sposób zarządzania nim znajduje się w załączniku nr 11,
   b) Struktura zbioru PEFS 2007 znajduje się w załączniku nr 18.
3) Pomost STD
   a) Zgodnie z §3 ust. 4 oraz §5 Rozporządzenia zestawienie struktur dokumentów elektronicznych w formacie XML, wraz z formatami danych oraz protokołami komunikacyjnymi i szyfrującymi udostępnia się razem z dokumentacją opisu systemu na stronie internetowej, której adres do wiadomości publicznej ogłasza Minister Pracy i Polityki Społecznej oraz w załączniku nr 9.
4) Płatnik
   a) Opis struktury danych osobowych wraz z ich przepływem znajduje się w załączniku nr 19.
5) Finanse
   a) Opis struktury zbioru danych osobowych znajduje się w załączniku nr 20.

§ 15

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych Ośrodek Pomocy Społecznej w Jastrzębiu-Zdroju stosować będzie środki techniczne i organizacyjne właściwe do bezpieczeństwa na poziomie wysokim zgodnie z Rozporządzeniem 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.

Zastosowano w szczególności:

1) Środki ochrony fizycznej danych:
   a) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C,
   b) Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy,
   c) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych,
   d) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony,
   e) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony,
   f) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie,
   g) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej,
   h) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy,
   i) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

2) Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,
b) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
c) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,
d) Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł,
e) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych,
f) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji,
g) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia,
h) Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii dysku twardego,
i) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,
j) Użyto system Firewall do ochrony dostępu do sieci komputerowej,
k) Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

3) Środki ochrony w ramach narzędzi programowych i baz danych:
a) Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych,
b) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych,
c) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
d) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych,
e) Zastosowano kryptograficzne środki ochrony danych osobowych,
f) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,
g) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

4) Środki organizacyjne:
   a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
   b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,
   c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
   d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
   e) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

5) Zabezpieczenie Obszaru

Obszar zabezpieczony będzie przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych; przebywanie osób nieuprawnionych w Obszarze, będzie dopuszczalne tylko za zgodą Dyrektora i w obecności osoby upoważnionej do przetwarzania danych osobowych.

Drzwi do pomieszczeń znajdujących się na terenie Obszaru zaopatrzone są w zamek kluczowy. Drzwi pozostawać będą zamknięte zarówno po czasie pracy Pracownika jak i w wypadku chwilowego opuszczenia przez niego pomieszczenia w ciągu dnia pracy. Przed opuszczeniem stanowiska klucz do drzwi pomieszczenia Pracownik zabiera ze sobą. Ekrany monitorów stanowisk dostępu do Danych osobowych będą automatycznie wyłączane po upływie 3 minut nieaktywności Pracownika. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do Danych Osobowych będą ustawione w sposób uniemożliwiający tym osobom wgląd w dane. Drzwi do serwerowni SA o podwyższonej odporności na włamanie.

Budynki są chronione, monitorowane, posiadają system alarmowy, a w czasie nieobecności pracowników nadzorowane są przez pracowników ochrony.

6) Mechanizmy kontroli dostępu do danych
   a) W systemie informatycznym stosowane będą następujące mechanizmy kontroli dostępu do danych osobowych:

i) Hasło do sieci wewnętrznej(domeny) Ośrodka Pomocy Społecznej, użytkownik ma obowiązek zmiany hasła nie rzadziej niż raz na 30 dni,

ii) Hasła do programów operujących na zbiorach danych osobowych.

b) Dostęp do danych będą miały wyłącznie osoby, których zakres obowiązków wymaga uzyskiwania danych – w zakresie pozostającym w związku z wykonywanymi przez te osoby obowiązkami. Dostęp do danych może mieć miejsce jedynie po podpisaniu przez Pracownika oświadczenia o zachowaniu poszczególnych danych w tajemnicy,

c) O dostępie poszczególnych osób do danych decydował będzie Administrator Bezpieczeństwa. W przypadku sporu pomiędzy Pracownikiem, a Administratorem Bezpieczeństwa co do dostępu do danych i/lub zakresu tego dostępu, Administrator Bezpieczeństwa przekaże sprawę do rozstrzygnięcia Dyrektorowi Ośrodka Pomocy Społecznej,

d) Jeżeli dostęp do danych przetwarzanych w systemie informatycznym będą posiadać co najmniej dwie osoby, wówczas:

i) W systemie tym rejestrowany będzie dla każdego użytkownika odrębny identyfikator,

ii) Dostęp do danych będzie możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia – sposób uwierzytelnienia określony jest w instrukcji.

7) Zabezpieczenie systemu informatycznego

System informatyczny jest zabezpieczony, w szczególności przed:

a) Działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego – poprzez oprogramowanie antywirusowe, antyszpiegowskie oraz firewall,

b) Utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej – poprzez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe przechowywane będą w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem i usuwane niezwłocznie po ustaniu ich użyteczności, kopie zapasowe sporządzane są w 1 egzemplarzu na zewnętrznym nośniku danych, wykorzystanie urządzeń typu UPS do podtrzymania zasilania,

c) Dostępem osób nieuprawnionych do przetwarzania danych w Systemie informatycznym poprzez:

i) Stosowanie zabezpieczeń przewidzianych w Instrukcji oraz Zasadach Polityki; osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązany będzie do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza Obszarem, w tym do stosowania środków ochrony kryptograficznej wobec przetwarzanych danych osobowych,

ii) Pozbawianie wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie a w przypadku gdy nie jest to możliwe, uszkadzanie w sposób uniemożliwiający ich odczytanie urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe, przeznaczonych do likwidacji, przekazania podmiotowi nieuprawnionemu do przetwarzania danych, naprawy – w tym ostatnim przypadku pozbawić się będzie wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie albo naprawić je pod nadzorem osoby upoważnionej przez administratora danych.

8) Czas przetwarzania i usuwania danych osobowych

a) Dane osobowe przechowywane są nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. W przypadku danych zbieranych na podstawie przepisów powszechnie obowiązujących czas przetwarzania danych osobowych określa jednolity rzeczowy wykaz akt oraz inne przepisy szczegółowe. Usuwanie winno wystąpić w przeciągu roku,

b) Nie podlegają ewidencjonowaniu nośniki papierowe, w szczególności notatki, kopie, projekty pism zawierające dane osobowe są usuwane najpóźniej z chwilą załatwienia sprawy, w związku z prowadzeniem której zostały sporządzone. Usuwanie danych osobowych na nośnikach papierowych dokonywane jest za pomocą niszczarek w pomieszczeniach stanowiących obszar przetwarzania danych osobowych,

c) Za zgodą Administratora Bezpieczeństwa Informacji możliwe jest usunięcie dokumentacji papierowej zawierającej dane osobowe poza obszarem przetwarzania danych osobowych.

i) Na podstawie umowy powierzenia przetwarzania danych osobowych, o której mowa w §4 niniejszej Polityki,

ii) Na terenie przedsiębiorstwa zajmującego się przetwórstwem papieru, o ile czynność ta dokonywana jest w obecności zatrudnionej przez Administratora Danych Osobowych osoby upoważnionej do przetwarzania danych osobowych w sposób uniemożliwiający zapoznanie się z danymi przez osoby postronne.

d) Z w/w czynności sporządzany jest protokół,

e) Zasady usuwania danych osobowych zapisanych na nośnikach elektronicznych reguluje Instrukcja zarządzania systemem informatycznym.

9) W pomieszczeniach przeznaczonych do przechowywania kopii zapasowych mogą przebywać wyłącznie:
   a) ABI,
   b) ASI,
   c) Osoby upoważnione przez ASI.

§ 16

Załączniki i ich udostępnianie.

1) Załącznikami do niniejszej polityki bezpieczeństwa są:
   a) Załącznik nr 1 - Wykaz budynków, pomieszczeń lub części pomieszczeń w których przetwarzane są dane osobowe,
   b) Załącznik nr 2 - Wzór upoważnienia do przetwarzania danych osobowych,
   c) Załącznik nr 3 - Wzór ewidencji upoważnień do przetwarzania danych osobowych,
   d) Załącznik nr 4 – wzór umowy o powierzenie danych osobowych,
   e) Załącznik nr 5 – rejestr osób upoważnionych do przetwarzania danych osobowych w zbiorze Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007,
   f) Załącznik nr 6 – oświadczenie uczestnika projektu,
   g) Załącznik nr 7 – wzór upoważnienia do przetwarzania danych osobowych na poziomie beneficjenta i podmiotów przez niego umocowanych,
   h) Załącznik nr 8 – wzór odwołania upoważnienia do przetwarzania danych osobowych na poziomie beneficjenta i podmiotów przez niego umocowanych,
   i) Załącznik nr 9 – opis przetwarzania danych w programie Pomost STD,
   j) Załącznik nr 10 – wzór wniosku o udostępnienie danych osobowych,
   k) Załącznik nr 11 – Instrukcja wypełniania Formularza PEFS 2007 dla PO KL,
   l) Załącznik nr 12 – rejestr osób uczestniczących w zebraniu dotyczący aktualizacji polityki bezpieczeństwa,
   m) Załącznik nr 13 - *UMOWA TRÓJSTRONNA nr It.1333.008.2014,*
   n) Załącznik nr 14 - Załącznik nr 6 do *UMOWY TRÓJSTRONNEJ nr It.1333.008.2014* stanowi osobną umowę dotyczącą przetwarzania danych osobowych przez firmę Sygnity S.A.,
   o) Załącznik nr 15 – umowa dotycząca zbioru PEFS 2007,
   p) Załącznik nr 16 – aneks do umowy dotyczącej zbioru PEFS 2007,

q) Załącznik nr 17 - ewidencja pracowników upoważnionych do przetwarzania danych osobowych w związku z wykonywaniem umowy ramowej w ramach Programu Operacyjnego Kapitał Ludzki,

r) Załącznik nr 18 - opis struktury zbioru PEFS 2007,

s) Załącznik nr 19 – opis przetwarzania danych w programie Płatnik,

t) Załącznik nr 20 – opis przetwarzania danych w programie Finanse,

u) Załącznik nr 21 – dokumentacja techniczna elektronicznego obiegu dokumentów EZD SIDAS,

v) Załącznik nr 22 – załączniki do dokumentacji technicznej elektronicznego obiegu dokumentów EZD SIDAS,

w) Załącznik nr 23 – umowa dotycząca na bazie, której powstał zbiór „REALIZACJA PROGRAMU AKTYWNY SAMORZĄD",

x) Załącznik nr 24 - świadectwo zgodności o nr 1/1.04/PS/GP/2015 dla systemu Pomost STD,

y) Załącznik nr 25 - bezpieczenstwo danych systemu SEPI,

z) Załącznik nr 26 - struktura danych osobowych SEPI.

2) Załącznik nr 1 udostępnia się wyłącznie:
   a) Osobom upoważnionym do przetwarzania danych osobowych,
   b) Osobom zatrudnionym na stanowiskach związanych z ochroną obiektów,
   c) Osobom, do których obowiązku należy sprzątanie obiektów.
3) Załączniki 2, 3, 4, 6, 7, 8, 12, 17 udostępnia się wyłącznie osobom upoważnionym do przetwarzania danych osobowych,
4) Osoby, które zostały zapoznane z załącznikami zobowiązane są do zachowania ich treści w tajemnicy,
5) Załącznik nr 9, 11, 13, 14 15, 16, 18, 19, 20, 21, 22, 23, 25, 26 udostępnia się wyłącznie osobom zatrudnionym na stanowisku informatyka w Ośrodku Pomocy Społecznej w Jastrzębiu-Zdroju,
6) Załącznik nr 10 udostępnia się osobom upoważnionym do przetwarzania danych osobowych oraz osobom, których dane osobowe dotyczą i przetwarzane są w zbiorze danych Ośrodka Pomocy Społecznej w Jastrzębiu-Zdroju,
7) Załączniki 5 i 17 udostępnia się osobom zajmującym się prowadzeniem projektów EFS oraz osobom zatrudnionym na stanowisku informatyka w Ośrodku Pomocy Społecznej w Jastrzębiu-Zdroju,
8) Załącznik nr 24 udostępnia się na wniosek osób zainteresowanych.

§ 17

Aktualizacja Polityki Bezpieczeństwa.

1. Niniejsza Polityka powinna być poddawana przeglądowi przez Administratora Bezpieczeństwa Informacji nie rzadziej niż raz do roku.
2. Treść Polityki jest aktualizowana w przypadku wprowadzenia lub zmiany środków technicznych lub organizacyjnych służących ochronie danych osobowych(zarówno w systemie informatycznym jak i danych przetwarzanych poza tym systemem np. w kartotekach papierowych)
3. Po dokonaniu aktualizacji tworzy się nową wersję Polityki nadając jej kolejny numer oraz organizuje się zebranie pracowników, na którym się udostępnia nową wersje do wglądu i omawia zmiany jakie zaszły. Wykaz osób uczestniczących w tym zebraniu jest ewidencjonowany w załączniku nr 13.

§ 18

Postanowienia końcowe

1. Zasady polityki bezpieczeństwa danych osobowych jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

§ 19

1. Dyrektor jest zobowiązany do zapoznania z treścią Instrukcji każdego użytkownika.
2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym iż został zaznajomiony z przepisami Ustawy oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
3. Wzór oświadczenia potwierdzające zaznajomienie użytkownika z przepisami Ustawy oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, stanowi załącznik nr 1 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 20

1. W sprawach nieregulowanych w niniejszej Instrukcji mają zastosowanie przepisy z Ustawy oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji.
3. Polityka wchodzi w życie z dniem jej podpisania.

DYREKTOR
Ośrodka Pomocy Społecznej
mgr Teresa [illegible]

.....

W imieniu Administratora Danych Osobowych

INSTRUKCJA

Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Jastrzębiu-Zdroju oraz Noclegowni

§ 1

Podstawa prawna

1. Paragraf 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024 z późn. zm.).

§ 2

Definicje

Ilekroć w instrukcji jest mowa o:

a) **Administratorze Danych Osobowych (ADO)** – rozumie się przez to Dyrektora Ośrodka Pomocy Społecznej w Jastrzębiu-Zdroju,
b) **Administratorze Bezpieczeństwa Informacji (ABI)** – rozumie się przez to soboę odpowiedzialną za bezpieczeństwo danych w systemie informatycznym, upoważnioną do pełnienia funkcji administratora przez Dyrektora Ośrodka Pomocy Społecznej,
c) **Dyrektorze** – rozumie się przez to Dyrektora Ośrodka Pomocy Społecznej w Jastrzębiu-Zdroju,
d) **Zasadach Polityki** – rozumie się przez to aktualne i zatwierdzone przez osobę działającą w imieniu Administratora Danych Osobowych - Zasady Polityki Bezpieczeństwa Danych Osobowych,
e) **Pracowniku** – rozumie się przez to pracownika Ośrodka Pomocy Społecznej zatrudnionego przy przetwarzaniu danych osobowych,
f) **Zbiorze danych** – 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,
g) **Przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
h) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
i) **Identyfikatorze Użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
j) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
k) **Uwierzytelnianiu** – rozumie się przez to działanie którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
l) **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
m) **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
n) **Osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowanie i jego konserwację** – rozumie się przez to informatyka odpowiedzialnego za powyższe zadania wyznaczone przez Dyrektora, zwanego dalej „Informatykiem",
o) **Poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom,

§ 3

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

a) Uprawnienia do przetwarzania danych nadaje poszczególnym Pracownikom Administrator Bezpieczeństwa Informacji, upoważniony przez Dyrektora Ośrodka Pomocy Społecznej, w oparciu o Zasady dostępu do danych, określone w Zasadach Polityki. Upoważnienie nie może być nadane bez uprzedniego złożenia przez Pracownika, w formie pisemnej, oświadczenia o obowiązku zachowania danych w tajemnicy,

b) Uprawnienia Pracowników do przetwarzania danych rejestrowane są w Systemie Informatycznym przez Administratora Bezpieczeństwa poprzez posiadanie indywidualnego identyfikatora umożliwiającego logowanie do tych aplikacji, z którymi może pracować. Administrator Bezpieczeństwa prowadzi Ewidencje osób zatrudnionych przy przetwarzaniu danych osobowych (stanowiącą załącznik nr 3 do Zasad Polityki Bezpieczeństwa),

c) Administrator bezpieczeństwa monitorował będzie wdrożone zabezpieczenia systemu informatycznego, nadzorował będzie oraz dokonywał okresowych kontroli przestrzegania przez Pracowników obowiązków zawartych w Instrukcji i Zasadach Polityki oraz obowiązujących przepisach prawa. W przypadku stwierdzenia nieprawidłowości przez Administratora Bezpieczeństwa niezwłocznie zwraca na nie uwagę Pracownikowi oraz informuje na piśmie przełożonego Pracownika, który kierując się wagą naruszenia zarządza podjęcie odpowiednich środków porządkowych i dyscyplinarnych w stosunku do Pracownika,

d) Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia i przedstawiania raportów z prowadzonej działalności w zakresie zarządzania Systemem informatycznym.

§ 4

1) Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

a) Każdy Pracownik posiada odrębny identyfikator, który zostaje mu nadany przez Administratora Bezpieczeństwa wraz z jego imieniem i nazwiskiem zostaje wpisany przez Administratora Bezpieczeństwa do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, prowadzonej przez Administratora Bezpieczeństwa i zarejestrowany przez Administratora Bezpieczeństwa w systemie informatycznym oraz posiada, wybrane przez siebie, odrębne Hasło, składające się co najmniej z 8 znaków,

b) Uwierzytelnianie dostępu Pracownika do danych w Systemie informatycznym następuje przez podanie hasła dostępu do sieci wewnętrznej(domeny) a następnie hasła dostępu do poszczególnych aplikacji dziedzinowych działających w tej sieci,

c) Pracownik zobowiązany jest zmieniać Hasło co 30 dni. Termin zmiany hasła wymuszany jest przez system uwierzytelniania użytkowników w sieci wewnętrznej(domenie). W aplikacjach dziedzinowych konieczność zmiany Hasła jest wymuszana lub sygnalizowana przez

odpowiedni komunikat. Identyfikator Pracownika nie powinien być zmieniany. Po wyrejestrowaniu Pracownika z systemu informatycznego ten sam identyfikator nie może być przydzielony innej osobie,

d) Podanie przez Pracownika hasła lub identyfikatora osobie nie upoważnionej stanowi ciężkie naruszenie podstawowych obowiązków pracowniczych i może stanowić podstawę do rozwiązania umowy o pracę bez wypowiedzenia.

§ 5

1) Procedury rozpoczęcia, zwiększenia i zakończenia pracy przez użytkowników Systemu informatycznego.

a) Przed rozpoczęciem pracy w Systemie informatycznym Pracownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych. W sytuacji gdy występuje konieczności zawieszenia pracy w systemie informatycznym Pracownik obowiązany jest postępować zgodnie z zasadami określonymi w Zasadach Polityki Bezpieczeństwa. Po zakończeniu pracy w Systemie informatycznym Pracownik wylogowuje się z systemu informatycznego, a następnie wyłącza sprzęt komputerowy oraz zabezpiecza stanowisko pracy,

b) W razie stwierdzenia przez Pracownika faktu naruszenia w jakikolwiek sposób bezpieczeństwa danych osobowych, lub chociażby powzięcia wątpliwości co do okoliczności, że takie naruszenie miało miejsce, Pracownik jest zobowiązany:

i. Niezwłocznie zabezpieczyć dowody potwierdzające naruszenie lub podejrzenie naruszenia zabezpieczeń Systemu informatycznego, a w szczególności: wszelką dokumentacje oraz nośniki magnetyczne, na których znajdują się dane osobowe,
ii. Niezwłocznie sporządzić pisemny raport zawierający opis stwierdzonego naruszenia lub istniejących wątpliwości z podaniem w treści raportu jaki stan urządzenia, zawartość zbioru danych, metody pracy, sposoby działania programu lub jakość komunikacji wskazują na naruszenie zabezpieczeń,
iii. Niezwłocznie powiadomić Administratora Bezpieczeństwa, osobiście, drogą fax'u lub telefonicznie o dokonanym naruszeniu (lub powstałych wątpliwościach) oraz: sposobie dokonania naruszenia, okolicznościach wskazujących na fakt zaistnienia naruszenia,
iv. W terminie 2 dni od dnia przekazania Administratorowi Bezpieczeństwa, Informacji, o której mowa w pkt. C), przekazać mu osobiście, lub w inny sposób, zapewniający zachowanie tajemnicy, pisemny raport, o którym mowa w pkt. b) – sposób przekazania raportu będzie każdorazowo uzgadniany pomiędzy Pracownikiem, a Administratorem Bezpieczeństwa.

§ 6

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

2) Kopie zapasowe sporządzane są przez wyznaczonych pracowników w każdy dzień roboczy i przechowywane na nośnikach optycznych

3) Administrator Bezpieczeństwa
   a) - sprawdza kopie zapasowe raz w miesiącu pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,

   b) - niezwłocznie usuwa kopie zapasowe po ustaniu ich użyteczności, pozbawiając je wcześniej zapisu danych osobowych, a gdy nie jest to niemożliwe – uszkadzając w sposób uniemożliwiający odczytanie.

§ 7

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

2. Kopie informatyczne oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępniania, mogą być przechowywane jedynie w zamkniętych szafach znajdujących się w pomieszczeniach na terenie Ośrodka.

3. Kopie zapasowe nie mogą być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco.

4. Kopie informatyczne oraz wydruki z danymi osobowymi przechowywane są przez 5 lat w przypadku klientów Ośrodka a dane osobowe pracowników 50 lat.

5. W przypadku projektów systemowych okres przechowywania kopii dokumentacji projektowej musi być tak długi jak projekt może być kontrolowany.

§ 8

1. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

2. Zainstalowana zapora ogniowa (firewall).

3. Zainstalowane oprogramowanie antywirusowe i antyszpiegowskie.

§ 9

Sposób informowania o odbiorcach danych.

System służący do przetwarzania danych osobowych zapewnia dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowanie:

- daty pierwszego wprowadzenia danych do systemu,
- identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
- źródła danych, w przypadku zbierania danych nie od osoby, której one nie dotyczą,
- informacji o odbiorcach, w rozumieniu ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używane jest do przetwarzania danych zawartych w zbiorach jawnych,
- odnotowanie informacji, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.

Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji następuje w formie tradycyjnej(papierowej) lub komputerowo poza systemem.

§ 10

1. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

2. Przegląd i konserwacja Systemu informatycznego i nośników informacji służących do przetwarzania danych odbywa się raz na miesiąc i przeprowadzany jest w obecności i pod nadzorem Administratora Bezpieczeństwa lub osoby przez niego upoważnionej.

3. W przypadku naprawy nośniki pozbawia się wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora Danych.

4. Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Administratora Bezpieczeństwa Informacji lub osoba przez niego wyznaczona.

§ 11

1. Wykaz zbiorów danych tworzących księgi rachunkowe na komputerowych nośnikach danych znajduje się w Polityce o rachunkowości Ośrodka Pomocy Społecznej w Jastrzębiu-Zdroju, ul. Opolska 9.
2. Opis systemu informatycznego przetwarzania danych księgowych prowadzonych przez Ośrodek Pomocy Społecznej w Jastrzębiu-Zdroju, ul. Opolska 9 znajduje się w załącznikach do Polityki o rachunkowości.

Postanowienia końcowe

§ 12

Instrukcja jest dokumentem wewnętrznym i nie może być udostępniana osobą postronnym w żadnej formie.

§ 13

1. Kierownicy Działów są zobowiązani do zapoznania z treścią instrukcji każdego użytkownika.
2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
3. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administrator Danych, a także o zobowiązaniu się do ich przestrzegania, stanowi załącznik nr 1 do Instrukcji.
4. Oświadczenia przechowywane są w aktach personalnych pracownika.

§ 14

1. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r., o ochronie danych osobowych (tj. Dz. U. z 2002r., Nr 101, poz. 926 z późn. zm.) oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej instrukcji.