Załącznik do Zarządzenia Nr 475/2018 Kierownika Ośrodka Pomocy Społecznej Gminy Lubawa z dnia 25 maja 2018 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa

Polityka Bezpieczeństwa Danych Osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa

PREAMBUŁA

Ośrodek Pomocy Społecznej Gminy Lubawa (zwany dalej Ośrodkiem) świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklaruje zamiar:

podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,

stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Ośrodku w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania świadomości wartości powierzonych Ośrodkowi danych osobowych jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodności Ośrodka,

traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,

doskonalenia i rozwijania nowoczesnych metod zabezpieczania danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.

Użyte w dokumencie określenia oznaczają:

1) **Administrator Danych Osobowych** – Kierownika Ośrodka Pomocy Społecznej Gminy Lubawa, zwanego dalej ADO;
2) **Inspektor Ochrony Osobowych** – osobę wyznaczoną przez ADO nadzorująca stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, zwaną dalej IOD;
3) **Administrator Systemów Informatycznych** – osobę wyznaczoną przez ADO, odpowiedzialną za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających zbiory danych osobowych, zwaną dalej ASI;
4) **Użytkownik systemu** – osobę posiadającą upoważnienie wydane przez ADO lub osobę upoważnioną do przetwarzania danych osobowych zgromadzonych w zbiorach danych osobowych oraz systemach informatycznych zastosowanych do ich przetwarzania, zwaną dalej użytkownikiem;
5) **Zbiór danych osobowych** –uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
6) **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); 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;
7) **Przetwarzanie danych** – oznacza 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;
8) **Zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
9) **Systemy informatyczne** – zbiór wszystkich programów i systemów informatycznych używanych w Ośrodku, dostępnych w lokalnej sieci komputerowej lub zainstalowanych na poszczególnych stacjach roboczych, za pomocą których są przetwarzane dane osobowe;
10) **System tradycyjny** – zespół procedur organizacyjnych (związanych z mechanicznym przetwarzaniem informacji), wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
11) **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

CZĘŚĆ I
Instrukcja Ochrony Danych Osobowych

ROZDZIAŁ 1
Przepisy ogólne i objaśnienia

§ 1

1. Polityka Bezpieczeństwa Danych Osobowych Ośrodka Pomocy Społecznej Gminy Lubawa jest zbiorem zasad i procedur obowiązujących przy zbieraniu, utrwalaniu, organizowaniu, porządkowaniu, przechowywaniu, adaptowaniu lub modyfikowaniu, pobieraniu, przeglądaniu, wykorzystywaniu, ujawnianiu poprzez przesłanie, rozpowszechnianiu lub innego rodzaju udostępnianiu, ograniczeniu, usuwaniu lub niszczeniu danych osobowych we wszystkich zbiorach.
2. Przetwarzanie danych osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa jest dopuszczalne tylko pod warunkiem przestrzegania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanej dalej RODO).

§ 2

Administrator Danych Osobowych zobowiązany jest do zapewnienia, aby dane osobowe były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów oraz przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne dla osiągniecia celu przetwarzania.

§ 3

1. Do realizacji postanowień niniejszej Polityki, Administrator Danych Osobowych wyznacza Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych.
2. Do zadań Inspektora ochrony danych należy:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia ogólnego;
   d) współpraca z Urzędem Ochrony Danych Osobowych;
   e) pełnienie funkcji punktu kontaktowego dla Urzędem Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

3. Do zadań Administratora Systemów Informatycznych należy w szczególności:
   a) zapewnienie optymalnej ciągłości działania systemu informatycznego,
   b) nadzór nad naprawami, konserwacją oraz likwidacja urządzeń komputerowych, na których zapisane są dane osobowe,
   c) nadawanie, zmiana i blokowanie uprawnień do systemów informatycznych,
   d) właściwa konfiguracja systemu informatycznego zapewniająca jego bezpieczeństwo i ograniczenie dostępu do danych osobowych przez osoby nieupoważnione,
   e) monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych,
   f) zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany,
   g) monitorowanie funkcjonowania zabezpieczeń nadzór nad czynnościami związanymi z prowadzeniem systemu sprawdzania oraz nadzorowanie wykonywanych procedur uaktualniania systemów antywirusowych i ich konfiguracji,
   h) podejmowanie działań w przypadku wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń lub podejrzenia naruszeń,
   i) nadzór nad wykorzystywanym oprogramowaniem oraz jego legalnością,
   j) nadzór nad wykonywaniem i przechowywaniem kopii zapasowych,
   k) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych.

ROZDZIAŁ 2
Gromadzenie i przetwarzanie danych osobowych

§ 4

1. Dane osobowe przetwarzane w Ośrodku mogą być uzyskiwane bezpośrednio od osób których dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.
2. Jeżeli przetwarzane odbywa się na podstawie zgody, osoba, której dane dotyczą musi dobrowolnie wyrazić zgodę na przetwarzanie swoich danych osobowych. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę.

§ 5

1. W przypadku zbierania danych osobowych od osoby, której dane dotyczą oraz w przypadku pozyskiwania ich w sposób inny niż od osoby, której dane dotyczą Administrator Danych Osobowych wypełnia obowiązek informacyjny.
2. Obowiązek informacyjny, o którym mowa w pkt.1 jest spełniony w sposób zwięzły, przejrzysty i zrozumiały, w łatwo dostępnej formie, jasnym i prostym językiem.

§ 6

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe nie mające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 7

1. W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora Danych Osobowych może on powierzyć ich przetwarzanie. Powierzenie przetwarzania odbywa się na podstawie umowy.
2. Administrator Danych Osobowych prowadzi Ewidencję podmiotów, którym powierza przetwarzanie danych. Wzór Ewidencji stanowi załącznik nr 1 do niniejszej Polityki.

§ 8

1. Inspektor Ochrony Danych prowadzi Rejestr czynności przetwarzania danych osobowych stanowiący załącznik nr 2 do niniejszej Polityki oraz sporządza Arkusz identyfikacji, oceny oraz określenia metod przeciwdziałania ryzyku stanowiący załącznik nr 3 do niniejszej Polityki.
2. Pracownicy poszczególnych działów/zespołów zgłaszają Inspektorowi Ochrony Danych zmiany dotyczące czynności przetwarzania danych osobowych w celu ich aktualizacji oraz wszystkie nowe czynności przetwarzania danych osobowych.
3. Pracownicy poszczególnych działów/zespołów zgłaszają Inspektorowi Ochrony Danych zagrożenia realizacji celów. Arkusz zgłoszenia ryzyka stanowi załącznik nr 4 do niniejszej polityki.
4. IOD prowadzi Rejestru kategorii czynności przetwarzania danych osobowych przetwarzanych w imieniu innego administratora stanowiący załącznik nr 5 do niniejszej Polityki.

§ 9

Ośrodek Pomocy Społecznej Gminy Lubawa nie przetwarza danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, chyba że osoba, której powyższe dane dotyczą wyraziła pisemną zgodę lub przetwarzanie to jest niezbędne do wypełnienia obowiązków wynikających z obowiązujące przepisy prawa.

§ 10

1. Osoby zaangażowane w procesie przetwarzania danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.
2. Osoby zaangażowane w procesie przetwarzania danych osobowych w systemach informatycznych są zobowiązane do postępowania zgodnie z „Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych”.

§ 11

1. Do przetwarzania danych osobowych są dopuszczeni jedynie osoby posiadające upoważnienie wydane przez ADO zgodnie z załącznikiem nr 6.
2. Osoby przetwarzający dane osobowe są zobowiązani do zachowania w tajemnicy danych osobowych do których mają dostęp w związku z wykonywanymi zadaniami służbowymi.
3. Nadanie upoważnienia do przetwarzania danych osobowych wymaga zaznajomienia się z przepisami dotyczącymi ochrony danych osobowych, w zakresie niezbędnym do czynności wykonywanych w ramach udzielonego upoważnienia.
4. Administrator Danych Osobowych jest odpowiedzialny za organizacje i przeprowadzenie szkoleń lub zaznajomienia osób upoważnionych z przepisami dotyczącymi ochrony danych osobowych.

5. Odbycie szkolenia z zakresu ochrony danych osobowych zostaje potwierdzone przez osobę w nim uczestniczącą w formie pisemnej. Wzór potwierdzenia uczestnictwa w szkoleniu stanowi załącznik nr 7 do niniejszej Polityki.

§ 12

Osoby przetwarzające dane są zobowiązane powiadomić IOD lub ASI o ewentualnych incydentach/naruszeniach bezpieczeństwa systemu ochrony danych osobowych we wszystkich zbiorach. Tryb postępowania określa „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych".

§ 13

Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe stanowi załącznik nr 8.

ROZDZIAŁ 3
Zbiory danych osobowych

§ 14

1. Pracownicy Ośrodka przetwarzający dane osobowe są zobowiązani do zgłoszenia Inspektorowi Ochrony Danych wszystkich informacji dotyczących powstania nowych zbiorów danych osobowych oraz wnoszenia zmian do zbiorów już istniejących. Wzór informacji o zbiorze danych osobowych stanowi załącznik nr 9 do niniejszej Polityki
2. ABI prowadzi wykaz zbiorów danych osobowych oraz systemów informatycznych zastosowanych do ich przetwarzania stanowiący załącznik nr 10 do niniejszej Polityki.

ROZDZIAŁ 4
Ochrona przetwarzania danych osobowych

§ 15

Administrator Danych Osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostepnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 16

Administrator danych osobowych ma obowiązek uwzględniania zagadnień ochrony danych osobowych, prywatności osób, których dane dotyczą oraz wdrożenia domyślnych ustawień prywatności już na etapie projektowania i opracowywania sposobów przetwarzania danych oraz w każdym kolejnym etapie przetwarzania.

§ 17

Środki techniczne ochrony danych osobowych:

1) pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),
2) pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w system alarmowy przeciwwłamaniowy,
3) pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolnostojącej gaśnicy,

4) dokumenty oraz nośniki elektroniczne zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 18

Środki organizacyjne ochrony danych osobowych:

1) pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w system alarmowy, który uruchamiany jest w momencie wykrycia ruchu po uzbrojeniu alarmu,
2) zapoznanie pracowników z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem ich do pracy przy przetwarzaniu danych osobowych,
3) przeszkolenie osób, o których mowa w pkt. 1 w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
4) zapoznanie pracowników z zasadą „czystego monitora" oraz zasadą „czystego biurka",
5) zapoznanie pracowników z technika trwałego niszczenia dokumentów,
6) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
7) stacje robocze, na których przetwarzane są dane osobowe posiadają zainstalowane oprogramowanie antywirusowe oraz zaporę firewall. Oprogramowanie na stacjach roboczych jest zawsze aktualne.
8) Użytkownicy aby mogli rozpocząć przetwarzanie danych w systemie informatycznym musza zalogować się do systemu podając unikalny login i hasło; hasło do systemu informatycznego, w którym przetwarzane są dane osobowe musi spełniać wymogi co do złożoności – zawierać co najmniej 8 znaków, małe i wielkie litery, znaki specjalne, cyfry; hasło musi być zmieniane nie rzadziej niż co 30 dni; po zakończeniu pracy w systemie użytkownik wylogowuje się z systemu,
9) podczas przerwy w pracy w systemie informatycznym i opuszczeniu stanowiska użytkownik blokuje stację roboczą w sposób uniemożliwiający kontynuację pracy bez wcześniejszego podania poświadczeń do systemu,
10) po upływie 15 minut bezczynności systemu, stacja robocza ulega samoczynnej blokadzie, aby kontynuować pracę w systemie użytkownik musi uwierzytelnić się do systemu poprzez podanie hasła,
11) dostęp do systemów informatycznych nadawany jest na podstawie upoważnień do przetwarzania danych osobowych; osoby zatrudnione przy przetwarzaniu danych osobowych otrzymują dostęp do systemów informatycznych umożliwiający im pracę w systemie oraz dostęp tylko do tych danych, do których zostały upoważnione.
12) konta osób, którym cofnięto upoważnienie do przetwarzania danych są blokowane w sposób uniemożliwiającym im zalogowanie się do systemu;
13) bazy danych systemów, w których przetwarzane są dane osobowe przechowywane są na serwerach; serwery baz danych umiejscowione są w serwerowni; dostęp do serwerowni ma tylko personel obsługi technicznej; serwerownia zabezpieczona jest przed nieautoryzowanym dostępem poprzez drzwi antywłamaniowe, pracownik uzyskuje dostęp do pomieszczenia poprzez autoryzację kartą chipową; serwerownia wyposażona jest w czujniki dymu, wilgotności, temperatury oraz ruchu. Po wykryciu nieprawidłowości uruchamiany jest system alarmowy; dane, które umieszczone są na serwerach zapisane są na macierzy dyskowej, dyski zabezpieczono stosując redundancję - system RAID 5.
14) kopie zapasowe operacyjnych systemów serwerowych, na których znajdują się bazy danych zawierające dane osobowe tworzone są codziennie i umieszczane na innej fizycznej macierzy dyskowej,

15) kopie zapasowe baz danych systemów, w których przetwarzane są dane osobowe wykonywane są codziennie i przechowywane na serwerze baz danych oraz dodatkowo na innej fizycznej macierzy dyskowej, dodatkowo tworzy się kopie zapasowe baz danych przed dokonywaniem kluczowych operacji na bazach danych – typu aktualizacja oprogramowania lub reindeksacja bazy.
16) na serwerach zainstalowane są systemy antywirusowe oraz zapory firewall,
17) logiczna infrastruktura sieci podzielona jest na sieci wirtualne, dostęp do wirtualnej sieci, w której znajdują się serwery jest ograniczony,
18) dostęp do sieci Internet kontroluje system IPS, który pełni funkcje routera, firewalla oraz systemu zapobiegania włamaniom do sieci. Ruch do sieci Internet oraz z sieci jest monitorowany i analizowany za pomocą procedur, które wykrywają potencjalne zagrożenie. Dostęp do nieodpowiednich treści jest zablokowany.

§ 19

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je do Prezesa Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzkiem naruszenia prawa lub wolności osób fizycznych.
2. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Ewidencja naruszeń bezpieczeństwa stanowi załącznik nr 11 do niniejszej Polityki.
3. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
4. Pracownicy Ośrodka Pomocy Społecznej Gminy Lubawa mają obowiązek niezwłocznie dokonać zgłoszenia naruszenia bezpieczeństwa ochrony danych osobowych, zgodnie z załącznikiem nr 12 do niniejszej Polityki.

§ 20

Zabezpieczenia danych osobowych w systemach informatycznych zostały opisane w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych”.

§ 21

Nadzór i kontrolę nad przestrzeganiem zasad ochrony danych osobowych realizuje IOD.

1. IOD jest zobowiązany do prowadzenia:
   a) ewidencji osób upoważnionych do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa, zgodnie z załącznikiem nr 13,
   b) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych.
2. W celu realizacji powierzonych zadań IOD ma prawo:
   a) kontrolować komórki organizacyjne w Ośrodku w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
   b) wydawać polecenia koordynatorom komórek organizacyjnych w zakresie bezpieczeństwa danych osobowych,
   c) żądania od wszystkich pracowników wyjaśnień w sytuacjach naruszeń bezpieczeństwa danych osobowych.

ROZDZIAŁ 5
Zasady udostępniania danych osobowych

§ 22

Administrator Danych Osobowych oraz inne upoważnione osoby tj. pracownicy Ośrodka udostępniają dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 23

1. Zbiory danych udostępnia się na pisemny, umotywowany wniosek, chyba, że odrębne przepisy prawa stanowią inaczej.
2. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
3. Wniosek jest rozpatrywany przez Administratora Danych Osobowych lub inną upoważnioną osobę.
4. Decyzje w sprawie udostępnienia podejmuje Administrator Danych Osobowych osobiście lub inna upoważniona osoba.
5. Rejestr udostępnionych danych osobowych stanowi załącznik nr 14.
6. W komórkach organizacyjnych Ośrodka prowadzone są na bieżąco w formie elektronicznej rejestry udostępnianych danych osobowych. Po zakończonym roku kalendarzowym rejestry przekazywane są do ABI.

§ 24

Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

CZĘŚĆ II
Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

ROZDZIAŁ 1
Przepisy ogólne i objaśnienia

§ 25

1. Instrukcja Zarządzania Systemami Informatycznymi, zwana dalej „Instrukcją" jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury używania, zarządzania i administrowania systemami informatycznymi służącymi do przetwarzania danych osobowych, wykorzystywanymi w Ośrodku Pomocy Społecznej Gminy Lubawa.
2. Instrukcja obejmuje swoim zakresem wszystkie osoby zatrudnione w Ośrodku, które biorą udział w procesie przetwarzania danych osobowych w systemach informatycznych.
3. Nieprzestrzeganie postanowień niniejszej instrukcji oraz brak nadzoru nad bezpieczeństwem informacji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej przepisami Kodeksu Pracy. Jeżeli skutkiem działania użytkownika jest ujawnienie informacji osobie nieupoważnionej, sprawca może być pociągnięty do odpowiedzialności karnej określonej przepisami Kodeksu Karnego. Jeżeli skutkiem działania użytkownika jest szkoda materialna, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego.
4. Polityka ustanawia procedury obowiązujące dla:
   a. Zbierania i przetwarzania danych osobowych przy użyciu systemu informatycznego,
   b. Powierzenia danych osobowych przetwarzanych przy użyciu systemu informatycznego upoważnionym podmiotom wewnętrznym i zewnętrznym,
   c. Uwierzytelniania dostępu podmiotów wewnętrznych i zewnętrznych do systemu informatycznego Podmiotu służącego do przetwarzania danych osobowych,
   d. Zapewnienia bezpieczeństwa systemu informatycznego i telekomunikacyjnego, wykorzystywanego przy przetwarzaniu danych osobowych przez podmiot,
   e. Zapewnienia bezpieczeństw zbiorów danych osobowych przetwarzanych przy użyciu systemu informatycznego,
   f. Korzystania z jednostki roboczej, sieci Internet i poczty e-mail przy użyciu systemu informatycznego Podmiotu,
   g. Zapewnienia bezpieczeństwa i korzystania z aplikacji stosowanych przy przetwarzaniu danych przy użyciu systemu informatycznego,
   h. Postepowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego.
5. Podmiot dochowuje należytej staranności przy zapewnianiu ochrony danych osobowych przetwarzanych w toku jego działalności w ramach systemu informatycznego którym się posługuje.
6. Przestrzeganie procedur ustanowionych w Instrukcji jest konieczne dla realizacji zasad zgodnego z prawem przetwarzania danych osobowych.

ROZDZIAŁ 2
Słowniczek

§ 26

Ilekroć w niniejszej Instrukcji jest mowa o:

1. Identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
2. Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3. Haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
4. Osobie upoważnionej – rozumie się przez to użytkownika systemu informatycznego uprawnionego do przetwarzania danych osobowych;
5. Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
6. Raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
7. Rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8. Uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

ROZDZIAŁ 3
Poziom bezpieczeństwa

§ 27

Poziom bezpieczeństwa systemów informatycznych przetwarzających dane osobowe określono jako wysoki. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną. Na bezpieczeństwo procesu przetwarzania danych osobowych składają się rozliczalność, poufność i integralność przetwarzanych danych.

1. Obszar, w którym przetwarza się dane osobowe zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2. Przebywanie osób nieuprawnionych w obszarze w którym przetwarza się dane osobowe jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
3. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
4. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
   a. W systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
   b. Dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
5. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się,

w szczególności przed:
   a. Działaniem oprogramowania, którego celem jest uzyskania nieuprawnionego dostępu do systemu informatycznego;
   b. Utrata danych spowodowana awarią zasilania lub zakłóceniami w sieci zasilającej.
6. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
7. W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielki litery oraz cyfry lub znaki specjalne. Hasła nie mogą zawierać loginu konta, do którego tworzone jest hasło, oraz innych informacji słownikowych.
8. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych osobowych.
9. Kopie zapasowe:
   a. Przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
   b. Usuwa się niezwłocznie po ustaniu ich użyteczności.
10. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarza się dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
11. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a. Likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   b. Przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   c. Naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
12. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
13. Zabezpieczenia logiczne, o których mowa w pkt. 12, obejmują:
   a. Kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
   b. Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.
14. Administrator Danych Osobowych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej.
15. Administrator Danych Osobowych monitoruje wdrożenie zabezpieczenia systemu informatycznego, stosując na poziomie wysokim środki bezpieczeństwa.
16. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych szczegółowo określone zostały w Polityce Bezpieczeństwa.

ROZDZIAŁ 4
Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemach informatycznych

§ 28

1. Każdy użytkownik przed przystąpieniem do przetwarzania danych zapoznaje się z Polityką Bezpieczeństwa Informacji w Ośrodku Pomocy Społecznej Gminy Lubawa oraz otrzymuje upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych.
2. Stosowany w Ośrodku schemat uprawnień zakłada, iż użytkownicy uzyskują dostęp do sieci komputerowej i do systemów informatycznych na z góry zdefiniowanym poziomie uprawnień użytkownika w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.
3. Rejestracji użytkowników w danym systemie dokonuje Administrator Systemów Informatycznych. Użytkownik po otrzymaniu od ASI informacji o założonym koncie z wymaganymi uprawnieniami, loguje się na nie w celu sprawdzenia poprawności otrzymanych informacji i uprawnień.
4. Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania danych osobowych lub rozwiązanie stosunku pracy lub umowy o innym charakterze obliguje ASI do odebrania temu użytkownikowi możliwości dostępu do danych osobowych przetwarzanych w systemach informatycznych.
5. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie jest usuwany z systemu informatycznego i nie jest przydzielany innej osobie.

ROZDZIAŁ 5
Metody i środki uwierzytelniania w systemach informatycznych oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 29

1. Do uwierzytelniania użytkownika podczas dostępu do sieci komputerowej i systemów informatycznych używa się identyfikatorów i haseł. Stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności – wszelkie działania w systemie przypisywane są konkretnemu użytkownikowi (nie dopuszcza się aby użytkownik korzystał z konta innego użytkownika),
2. Hasło użytkownika musi składać się z minimum 8 znaków, w tym minimum jedna wielka litera i jedna cyfra lub znaki specjalne.
3. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: identyfikatorów, dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych słów bezpośrednio kojarzących się z użytkownikiem.
4. Hasło nie może być ujawnione innej osobie nawet po utracie jego ważności.
5. Użytkownik musi zmieniać hasło nie rzadziej, niż raz na 30 dni.
6. Hasło przy wpisywaniu nie może być w sposób jawny wyświetlane na ekranie.
7. Obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu.
8. Użytkownik ponosi pełną odpowiedzialność za wszystkie operacje wykonane przy użyciu jego

identyfikatora i hasła dostępu.

9. Hasła administracyjne zapisane są za pomocą dedykowanego oprogramowania i zaszyfrowane. Klucz oraz hasło do rozszyfrowania haseł administracyjnych przechowywany jest w sejfie.

ROZDZIAŁ 6
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów

§ 30

1. Dostęp użytkowników do zasobów sieci komputerowej Ośrodka jest ograniczony, ze względu na czas i sytuacje opisane w Regulaminie Pracy Ośrodka.
2. Podczas rozpoczęcia pracy w sieci komputerowej użytkownik jest autoryzowany poprzez podanie swojego identyfikatora i hasła. Dopiero po pomyślnej autoryzacji w sieci komputerowej użytkownik może uzyskać możliwość uruchomienia programu służącego do przetwarzania danych osobowych, dokonując osobnej autoryzacji w tym programie.
3. Przy każdorazowym opuszczeniu stanowiska komputerowego, użytkownik jest zobowiązany dopilnować, aby na ekranie nie były wyświetlane informacje lub dane osobom nieuprawnionym, poprzez:
   a) zablokowanie komputera odpowiednią kombinacją klawiszy, lub
   b) stosowanie wygaszacza ekranu zabezpieczonego hasłem, lub
   c) wylogowanie się z sieci komputerowej.
4. Użytkownik jest zobowiązany do zadbania, aby niemożliwe było odczytanie informacji z monitora przez osoby nieuprawnione.
5. Podczas kończenia pracy na danej stacji roboczej należy:
   a) wylogować się z systemu informatycznego,
   b) wylogować się z sieci komputerowej, zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
   c) sprawdzić czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.
6. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonane czynności aż do momentu rozliczenia ze sprzętu komputerowego.
7. W sytuacji naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego, użytkownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie ABI lub ASI.

ROZDZIAŁ 7
Procedury tworzenia kopii zapasowych zbiorów danych

§ 31

1. W celu zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych Ośrodka, przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach Ośrodka w oparciu o architekturę klient-serwer. Wynika stąd praktyka przetwarzania danych w bazach znajdujących się na dedykowanych dla poszczególnych programów, serwerach. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy Ośrodka, stanowią jedynie końcówki klienckie systemu.
2. Wszelkie informacje (w tym dane osobowe), przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach systemów informatycznych, są zapisywane bezpośrednio na serwerach.

§ 32

3. Kopie zapasowe w formie kopii pełnych baz danych zlokalizowanych na serwerach wykonane są w cyklu dobowym, poza godzinami pracy Ośrodka, za pomocą skryptów archiwizujących, uruchamianych automatycznie o określonych porach.
4. Kopie zapasowe wykonywane są każdorazowo przed wykonaniem aktualizacji w systemach informatycznych i bazodanowych a także przed wykonywaniem prac konserwacyjnych systemów.
5. ASI sprawuje nadzór nad wykonywaniem w/w kopii zapasowych oraz weryfikuje ich poprawność.
6. Kopie zapasowe baz danych zapisywane są na:
   a) dysku twardym serwera oraz na zewnętrznej macierzy dyskowej (serwerownia, budynek B Urzędu Gminy Lubawa),
7. Kopie zapasowe dokumentów wytworzonych przez użytkowników znajdujące się w folderze „Moje Dokumenty" oraz „Pulpit" są wykonywane automatycznie bez ingerencji użytkowników. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów, które nie znajdują się w w/w folderach.

ROZDZIAŁ 8
Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 33

1. Elektroniczne nośniki informacji:
   a) dane w postaci elektronicznej przetwarzane w systemie zapisane na nośnikach materialnych (płytach CD\DVD, pamięciach przenośnych czy dyskach twardych) są własnością Ośrodka,
   b) w/w elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych,
   c) po zakończeniu pracy przez użytkownika systemu informatycznego, w/w elektroniczne nośniki informacji są przechowywane w meblach biurowych,
   d) elektroniczne nośniki informacji, o których mowa powyżej powinny być oznaczone w sposób umożliwiający ich identyfikację.
2. Przekazywanie i niszczenie elektronicznych nośników informacji:
   a) elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez Administratora Danych Osobowych,
   b) dane osobowe na każdym nośniku zewnętrznym powinny być zabezpieczone przed odczytem (minimum hasłem),
   c) dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych,
   d) przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu podpisanego przez ADO, ABI oraz właściwych użytkowników.
3. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.

ROZDZIAŁ 9
Środki ochrony systemów informatycznych przed tzw. „szkodliwym oprogramowaniem” oraz próbami dostępu przez osoby nieuprawnione

§ 34

1. ASI odpowiada za ochronę antywirusową i wykonuje czynności związane z ochroną antywirusową, wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego.
2. Oprogramowanie antywirusowe jest instalowane centralnie na serwerze oraz na wszystkich stanowiskach komputerowych podłączonych do sieci.
3. Aktualizacja oprogramowania antywirusowego odbywa się w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci komputerowej.
4. Użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów lub szkodliwego oprogramowania.
5. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki.
6. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

§ 35

7. ASI jest odpowiedzialny za aktywowanie i poprawną konfigurację specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   a) sieci lokalnej i sieci zewnętrznej,
   b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
8. ASI obowiązany jest do utrzymywania stałej aktywności zainstalowanego specjalistycznego oprogramowania monitorującego wymianę danych oraz do jego aktualizacji.

ROZDZIAŁ 10
Procedury wykonywania przeglądów i konserwacji sprzętu oraz systemów informatycznych

§ 36

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację fizycznej platformy sprzętowej, na której eksploatowane są systemy informatyczne.
2. Przeglądy i konserwację urządzeń wchodzących w skład platformy sprzętowej wykonuje się w terminach określonych przez producenta sprzętu. W przypadku gdy producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych lub też nie określił ich częstotliwości, o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje ASI.
3. Nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, muszą być niezwłocznie usunięte, a ich przyczyny przeanalizowane przez ASI.
4. Przegląd systemów informatycznych i narzędzi programistycznych przeprowadzany jest przez ASI, w celu sprawdzenia poprawności ich działania i wykonywany jest w następujących przypadkach:

a) zmiany wersji oprogramowania systemu informatycznego lub operacyjnego na danym stanowisku komputerowym,
b) wykonania zmian w systemie informatycznym spowodowanych koniecznością naprawy lub modyfikacji systemu.

5. Użytkownik ma obowiązek niezwłocznie powiadomić IOD o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
6. W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia podejrzenia możliwości uszkodzenia informacji Administrator Systemów Informatycznych w porozumieniu z IOD jest zobowiązany do:
   a) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,
   b) sprawdzenia spójności i integralności informacji przetwarzanych w systemie informatycznym,
   c) ocenić zasadność odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej,
   d) w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej.
7. W przypadku przekazywania do napraw urządzeń informatycznych służących do przetwarzania danych osobowych:
   a. Jeśli uszkodzenie nie dotyczy nośników pamięci, należy je wymontować i do naprawy przekazać urządzenie nie zawierające nośników, na których są dane osobowe.
   b. Jeśli uszkodzenie dotyczy nośników pamięci, należy zniszczyć je, przywracając pliki zawierające dane osobowe z kopii zapasowej.
   c. Jeśli uszkodzenie dotyczy nośników pamięci a jednocześnie a jednocześnie brak jest plików zawierających dane osobowe, wówczas należy zrealizować naprawę pod bezpośrednim nadzorem osoby upoważnionej albo po zawarciu umowy powierzenia danych osobowych.

ROZDZIAŁ 11
Dostęp zdalny do systemów informatycznych Ośrodka

§ 37

1. Pod pojęciem zdalnego dostępu do systemów informatycznych rozumie się połączenie z systemem informatycznym Ośrodka z lokacji znajdującej się poza siedzibą.
2. Zdalnego połączenia z systemem informatycznym Ośrodka mogą dokonać wyłącznie osoby do tego upoważnione.
3. System, z którego osoba upoważniona dokonuje dostępu zdalnego powinien posiadać odpowiednie zabezpieczenia i odpowiadać wymogom systemów używanych przy przetwarzaniu danych osobowych.

ROZDZIAŁ 12
Postanowienia końcowe

§ 38

1. Instrukcja zarządzania systemem informatycznym stanowi integralną część Polityki Bezpieczeństwa i jest dokumentem obowiązującym Podmiot w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.

2. Instrukcja zarządzania systemem informatycznym jest dokumentem obowiązującym wszystkie osoby dopuszczone do przetwarzania danych osobowych w ramach działalności podmiotu.
3. Każda osoba dopuszczona do przetwarzania danych osobowych w ramach działalności Podmiotu ma obowiązek zapoznania się z niniejszą Instrukcją zarządzania systemem informatycznym.
4. Naruszenie zasad wynikających z Polityki Bezpieczeństwa Danych Osobowych oraz z Instrukcji zarządzania systemem informatycznym może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia.
5. Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego

CZĘŚĆ III
Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

ROZDZIAŁ 1
Opis zdarzeń naruszających ochronę danych osobowych

§ 38

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, zalania, ogień, przerwy w zasilaniu w energię elektryczną, zwarcia i przepięcia w sieci elektroenergetycznej). Ich występowanie może prowadzić do utraty integralności danych, ich uszkodzenia, zniszczenia, uszkodzenia systemów komputerowych oraz elementów technicznych komputera lub sieci. Ciągłość systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych,
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, działanie wirusów). Może dojść do zniszczenia danych, zakłócenia ciągłości pracy systemu lub naruszenia poufności danych,
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na:
   - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
   - nieuprawniony dostęp do systemu z jego wnętrza,
   - nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie składników technicznych systemu.

§ 39

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe to:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzenie próby modyfikacji danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) niedopuszczalna manipulacja danymi osobowymi w systemie,

9) ujawnienie osobom nieupoważnionym danych osobowych, objętych tajemnicą procedur ochrony przetwarzania lub innych strzeżonych elementów zabezpieczeń systemu,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy, co świadczy o przełamaniu lub zaniechaniu ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu do sieci lub komputera, itp.,
11) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. "luk w systemie", itp.,
12) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia oraz skasowanie lub skopiowanie w sposób niedozwolony danych osobowych,
13) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie z programu, systemu przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

§ 40

1. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. papier (wydruki), dyskietki, płyty CD/DVD w formie niezabezpieczonej itp.

ROZDZIAŁ 2
Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 41

1. Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie IOD i/lub ASI w przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) jakości transmisji danych w sieciach komputerowych mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie pomieszczeń, pożar, itp.).
2. W razie niemożliwości zawiadomienia IOD i/lub ASI należy powiadomić Administratora Danych Osobowych.
3. Wzór zgłoszenia naruszenia bezpieczeństwa ochrony danych osobowych stanowi załącznik nr 12 do niniejszej Polityki.

§ 42

Czynności podejmowane przez IOD i/lub ASI w przypadku stwierdzenia naruszenia ochrony danych osobowych:

1) poinformowanie osoby zgłaszającej o dalszym trybie postępowania oraz zlecenie jej właściwego wykonywania czynności,
2) podjęcie czynności niezbędnych dla powstrzymania niepożądanych skutków zaistniałego

naruszenia oraz w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,

3) ustalenie czasu trwania i charakteru naruszenia, w miarę możliwości określić kategorie i przybliżoną liczbę osób, których dotyczy naruszenie,
4) ustalić możliwe konsekwencje naruszenia ochrony danych osobowych,
5) zarekomendować działania zapobiegawcze w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
6) w przypadku naruszenia ochrony danych osobowych, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – dokonać zgłoszenia do Prezesowi Urzędu Ochrony Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia),
7) w razie konieczności zainicjowanie działań dyscyplinarnych,
8) udokumentowanie prowadzonego postępowania w rejestrze naruszeń bezpieczeństwa danych osobowych stanowiącym załącznik nr 10 do niniejszej Polityki.

Kierownik
Ośrodka Pomocy Społecznej
Gminy Lubawa

/-/ Adam Roznerski