Załącznik do Zarządzenia Nr 219/2012 Kierownika Ośrodka Pomocy Społecznej Gminy Lubawa z dnia 25 czerwca 2012 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Ośrodka Pomocy Społecznej Gminy Lubawa

Polityka Bezpieczeństwa Informacji 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) **Ustawa** – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);
3) **Administrator Bezpieczeństwa Informacji** – osobę wyznaczoną przez ADO odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych zbiorach danych osobowych oraz w systemach informatycznych, zwaną dalej ABI;
4) **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;
5) **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;
6) **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
7) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
8) **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych takie jak: zbieranie, utrwalanie, opracowywanie, zmienianie, przechowywanie, analizowanie, raportowanie, aktualizowanie, udostępnianie lub usuwanie;
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 Informacji Ośrodka Pomocy Społecznej Gminy Lubawa jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach.
2. Przetwarzanie danych osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa jest dopuszczalne tylko pod warunkiem przestrzegania Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i wydanych na jej podstawie przepisów wykonawczych.

§ 2

Administrator Danych Osobowych zobowiązany jest do zapewnienia, aby dane osobowe były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów oraz merytorycznie poprawne i adekwatne w stosunku do celów.

§ 3

1. Do realizacji postanowień niniejszej Instrukcji, Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych.
2. Do zadań Administratora Bezpieczeństwa Informacji należy w szczególności:
   a) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe
   b) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych,
   c) prowadzenie ewidencji wydanych upoważnień i oświadczeń,
   d) nadzór nad obiegiem i przechowywaniem dokumentów zawierających dane osobowe,
   e) nadzór nad wykorzystywanym oprogramowaniem oraz jego legalnością,
   f) nadzór i kontrola ASI oraz pozostałych upoważnionych pracowników do przetwarzania danych osobowych.
3. Do zadań Administratora Systemów Informatycznych należy w szczególności:
   a) nadzór nad naprawami, konserwacją oraz likwidacja urządzeń komputerowych, na których zapisane są dane osobowe,
   b) zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany,
   c) nadzór nad czynnościami związanymi z prowadzeniem systemu sprawdzania oraz nadzorowanie wykonywanych procedur uaktualniania systemów antywirusowych i ich konfiguracji,
   d) nadzór nad wykonywaniem i przechowywaniem kopii zapasowych,
   e) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych.

ROZDZIAŁ 2
Gromadzenie i przetwarzanie danych osobowych

§ 4

Dane osobowe przetwarzane w Ośrodku mogą być uzyskiwane bezpośrednio od osób których dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 5

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.
3.

§ 6

1. Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe stanowi załącznik nr 1.
2. Wykaz zbiorów danych osobowych oraz systemów informatycznych zastosowanych do ich przetwarzania w Ośrodku stanowi załącznik nr 2.

§ 7

3. 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.
4. 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".

§ 8

1. Do przetwarzania danych osobowych są dopuszczeni jedynie pracownicy posiadający upoważnienie wydane przez ADO zgodnie z załącznikiem nr 3.
2. Pracownicy przetwarzający dane osobowe są zobowiązani do zachowania w tajemnicy danych osobowych do których mają dostęp w związku z wykonywanymi zadaniami służbowymi i obowiązkami pracowniczymi. Wzór oświadczenia stanowi załącznik nr 4.
3. Do przetwarzania danych osobowych Beneficjentów Ostatecznych (uczestników) projektów, w tym także w ramach Programu Operacyjnego Kapitał Ludzki współfinansowanych ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego otrzymują upoważnienie do przetwarzania tych danych oraz upoważnienie dostępu do formularza PEFS 2007 w zakresie POKL, zgodnie z wytycznymi Instytucji Zarządzającej POKL.

§ 9

Osoby przetwarzające dane są zobowiązane powiadomić ABI 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".

§ 10

Zabrania się przetwarzania danych ujawniających: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, przynależność partyjną lub związkową, stan zdrowia, kod genetyczny, nałogi lub fakty z życia seksualnego, skazania, orzeczenia o ukaraniu i inne orzeczenia wydane w postępowaniu sądowym lub

administracyjnym, chyba że pozwalają na to obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła pisemną zgodę.

ROZDZIAŁ 3
Rejestracja zbiorów danych osobowych

§ 11

Pracownicy Ośrodka przetwarzający dane osobowe są zobowiązani do zgłoszenia Administratorowi Bezpieczeństwa Informacji planowanego rejestrowania nowych zbiorów danych osobowych oraz wnoszenia zmian do zbiorów już zarejestrowanych.

ROZDZIAŁ 4
Ochrona przetwarzania danych osobowych

§12

ABI zobowiązany jest do stosowania środków organizacyjnych i technicznych zapewniających ochronę przetwarzania danych, w szczególności przed ich udostępnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione.

§ 13

Środki techniczne ochrony danych osobowych:

1) pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),
2) okna w pomieszczeniach w których przetwarzane są dane osobowe, zabezpieczone są za pomocą krat i rolet,
3) pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w system alarmowy przeciwwłamaniowy,
4) pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolnostojącej gaśnicy,
5) dokumenty oraz nośniki elektroniczne zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 14

Środki organizacyjne ochrony danych osobowych:

1) zapoznanie pracowników z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem ich do pracy przy przetwarzaniu danych osobowych,
2) przeszkolenie osób, o których mowa w pkt. 1 w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
3) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
4) zapoznanie pracowników z zasadą „czystego monitora" oraz zasadą „czystego biurka",
5) zapoznanie pracowników z technika trwałego niszczenia dokumentów.

§ 15

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

§ 16

1. Nadzór i kontrolę nad przestrzeganiem zasad ochrony danych osobowych realizuje ABI.
2. ABI jest zobowiązany do prowadzenia:

a) ewidencji wydanych upoważnień i oświadczeń osób przetwarzających dane osobowe, zgodnie z załącznikiem nr 5,
b) ewidencji osób, którym nadano i odebrano upoważnienia do przetwarzania danych osobowych Beneficjentów Ostatecznych (uczestników) projektów, w tym także w ramach Programu Operacyjnego Kapitał Ludzki współfinansowanych ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego oraz rejestru osób upoważnionych do przetwarzania danych osobowych w formularzu PEFS 2007 w zakresie POKL, zgodnie z wytycznymi Instytucji Zarządzającej POKL.

3. W celu realizacji powierzonych zadań ABI 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

§ 17

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.

§ 18

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 inna upoważniona osoba.
4. Decyzje w sprawie udostępnienia podejmuje Administrator Danych Osobowych osobiście lub inna upoważniona osoba.

§ 19

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

§ 1

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.

ROZDZIAŁ 2
Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemach informatycznych

§ 2

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 3
Metody i środki uwierzytelniania w systemach informatycznych oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 3

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 kont: administrator, gość, a także z konta innego użytkownika),
2. Hasło użytkownika musi składać się z minimum 8 znaków, w tym minimum jedna wielka litera i jedna cyfra.
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 w miesiącu.
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.

ROZDZIAŁ 4
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów

§ 4

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 5
Procedury tworzenia kopii zapasowych zbiorów danych

§ 5

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.

§ 6

1. 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.
2. Kopie zapasowe wykonywane są każdorazowo przed wykonaniem aktualizacji w systemach informatycznych i bazodanowych.
3. ASI sprawuje nadzór nad wykonywaniem w/w kopii zapasowych oraz weryfikuje ich poprawność.
4. Kopie zapasowe zapisywane są na dysku twardym serwera, na zewnętrznej macierzy dyskowej oraz na dysku twardym komputera znajdującego się w osobnym pomieszczeniu (Budynek E Urzędu Gminy Lubawa) i będącego pod bezpośrednim nadzorem ASI.
5. 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 6
Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 7

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 7
Środki ochrony systemów informatycznych przed tzw. „szkodliwym oprogramowaniem" oraz próbami dostępu przez osoby nieuprawnione

§ 8

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.

§ 9

1. 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.
2. ASI obowiązany jest do utrzymywania stałej aktywności zainstalowanego specjalistycznego oprogramowania monitorującego wymianę danych oraz do jego aktualizacji.

ROZDZIAŁ 8
Procedury wykonywania przeglądów i konserwacji sprzętu oraz systemów informatycznych

§ 10

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 Administratora Bezpieczeństwa Informacji 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 Administratorem Bezpieczeństwa Informacji 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.

CZĘŚĆ III
Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

ROZDZIAŁ 1
Opis zdarzeń naruszających ochronę danych osobowych

§ 1

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.

§ 2

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.).

§ 3

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

§ 4

Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie ABI 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.).

W razie niemożliwości zawiadomienia ABI i/lub ASI należy powiadomić Administratora Danych Osobowych.

§ 5

Czynności podejmowane do czasu przybycia ABI i/lub ASI na miejsce naruszenia ochrony danych osobowych:
1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub jego zastępcy.

§ 6

Czynności podejmowane przez ABI i/lub ASI po przybyciu na miejsce naruszenia ochrony danych osobowych:

1) zapoznanie się z zaistniałą sytuacją i dokonanie wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Ośrodka,
2) żądanie dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym zdarzeniem naruszenia ochrony danych,
3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu ADO. Jeżeli taka potrzeba istnieje, nawiązuje kontakt ze specjalistami.

§ 7

1. ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 8, który, powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   2) określenie czasu, miejsca naruszenia i powiadomienia,
   3) określenie okoliczności towarzyszących i rodzaju naruszenia,
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn wystąpienia naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
2. Raport o którym mowa w pkt 1 ABI niezwłocznie przekazuje Administratorowi Danych Osobowych, a w przypadku jego nieobecności osobie uprawnionej.
3. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii bezpieczeństwa oraz określa termin wznowienia przetwarzania danych (jeśli jest to możliwe).
4. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Ośrodka i ABI.
5. Analiza, o której mowa w pkt 4, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Załącznik Nr 1 do Polityki Bezpieczeństwa Informacji w Ośrodku Pomocy Społecznej Gminy Lubawa

WYKAZ BUDYNKÓW I POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

L.P.	MIEJSCE
1.	Budynek B Urzędu Gminy Lubawa, parter pok. nr 16 - Dział Finansowo-Księgowy
2.	Budynek B Urzędu Gminy Lubawa, parter pok. nr 17 - Dział Finansowo-Księgowy; Dział Organizacyjny
3.	Budynek B Urzędu Gminy Lubawa, parter pok. nr 18 - Kierownik Ośrodka
4.	Budynek B Urzędu Gminy Lubawa, parter pok. nr 19 - Dział Pomocy Środowiskowej Sekcja administracyjna
5.	Budynek B Urzędu Gminy Lubawa, parter- Serwerownia
5.	Budynek B Urzędu Gminy Lubawa, część piwniczna pok. nr 3 - Dział Pomocy Środowiskowej Zespół pracy socjalnej i integracji społecznej
6.	Budynek B Urzędu Gminy Lubawa, część piwniczna pok. nr 4 - Dział Świadczeń Społecznych
7.	Budynek B Urzędu Gminy Lubawa, część piwniczna - Składnica akt
8.	Budynek E Urzędu Gminy Lubawa - Dział Organizacyjny
9.	Budynek przy ul. 19-go stycznia 25, I piętro pok. nr 4 - Dział Programów i Projektów

Załącznik Nr 2 do Polityki Bezpieczeństwa Informacji w Ośrodku Pomocy Społecznej Gminy Lubawa

WYKAZ ZBIORÓW DANYCH OSOBOWYCH ORAZ SYSTEMÓW INFORMATYCZNYCH ZASTOSOWANYCH DO ICH PRZETWARZANIA

L.P.	NAZWA ZBIORU	NAZWA SYSTEMU	UWAGI
1.	Baza danych wnioskodawców ubiegających się o przyznanie zasiłku z systemu pomocy społecznej	POMOST STD	
2.	Fundusz alimentacyjny oraz dłużnicy alimentacyjni	FUNDUSZ ALIMENTACYJNY I ŚWIADCZENIA RODZINNE	
3.	Świadczenia rodzinne	FUNDUSZ ALIMENTACYJNY I ŚWIADCZENIA RODZINNE	
4.	Dodatki mieszkaniowe	DODATKI MIESZKANIOWE	
5.	Rodziny korzystające ze wsparcia i systemu pieczy zastępczej	POMOST STD	
5.	Ewidencja osób nadużywających alkohol	brak	
8.		PUMA	Platforma Uruchomieniowa Modułów Aplikacyjnych służy do wspomagania działu finansowo-księgowego w zakresie księgowości budżetowej oraz do realizacji zadań związanych z zatrudnieniem pracowników i ich wynagrodzeniem oraz do obsługi dokumentów ubezpieczeniowych i wymiany informacji z Zakładem Ubezpieczeń Społecznych i Urzędem Skarbowym.
9.		PŁATNIK	Baza danych płatników składek służąca do obsługi dokumentów ubezpieczeniowych, rozliczeniowych i wymiany informacji z Zakładem Ubezpieczeń Społecznych.
9.		OKRESOWA OCENA KWALIFIKACYJNA PRACOWNIKA SAMORZADOWEGO	Baza danych pracowników służąca do wypełniania arkusza oceny okresowej pracowników.
		PEFS 2007	Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 - zbiór danych osobowych Beneficjentów Ostatecznych (uczestników) projektów, w tym także w ramach Programu Operacyjnego Kapitał Ludzki współfinansowanych ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Załącznik Nr 3 do Polityki Bezpieczeństwa Informacji w Ośrodku Pomocy Społecznej Gminy Lubawa

Fijewo, dnia .....

UPOWAŻNIENIE
[nr upoważnienia]

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, ze zm.) upoważniam Panią/Pana

[imię i nazwisko]
[stanowisko]

do przetwarzania danych osobowych zgromadzonych w zbiorze danych osobowych oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład

L.P.	NAZWA ZBIORU	POSTAĆ ZBIORU	NAZWA SYSTEMU	IDENTYFIKATOR
1.	[nazwa zbioru]	papierowa/ elektroniczna	[nazwa systemu]	[identyfikator]

na okres **[okres]** w Ośrodku Pomocy Społecznej Gminy Lubawa.

.....
(Administrator Danych Osobowych)

Przyjęłam/Przyjąłem do wiadomości i stosowania

.....
(Data i podpis pracownika)

Załącznik Nr 4 do Polityki Bezpieczeństwa Informacji w Ośrodku Pomocy Społecznej Gminy Lubawa

Fijewo, dnia .....

OŚWIADCZENIE

Ja, niżej podpisana(y), zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam/będę miał(a) dostęp w związku z wykonywaniem przeze mnie obowiązków służbowych i obowiązków pracowniczych w Ośrodku Pomocy Społecznej Gminy Lubawa, zarówno w trakcie obecnie wiążącego mnie stosunku pracy jak i po ustaniu zatrudnienia.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Ośrodku Pomocy Społecznej Gminy Lubawa wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał(a) danych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

.....
(Podpis)

Załącznik Nr 5 do Polityki Bezpieczeństwa Informacji w Ośrodku Pomocy Społecznej Gminy Lubawa

EWIDENCJA WYDANYCH UPOWAŻNIEŃ I OŚWIADCZEŃ

L.P.	IMIĘ I NAZWISKO	NUMER UPOWAŻNIENIA	NAZWA ZBIORU	NAZWA SYSTEMU	IDENTYFIKATOR W SYSTEMIE	DATA NADANIA	DATA USTANIA

Załącznik Nr 6 do Polityki Bezpieczeństwa Informacji w Ośrodku Pomocy Społecznej Gminy Lubawa

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

1. Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

.....

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

5. Podjęte działania:

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

(Data i podpis Administratora Bezpieczeństwa Informacji)