Załącznik Nr 2
do Zarządzenia Nr 25/2017
Wójta Gminy Leszno
z dnia 1 marca 2017 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY LESZNO

LESZNO, MARZEC 2017 r.

WÓJT
Andrzej Cieślak

.....

Zatwierdził:

Administrator Danych Osobowych

1. **Wstęp**

Instrukcja stanowi zestaw procedur opisujących zasady zapewnienia bezpieczeństwa danych osobowych w systemach i aplikacjach informatycznych.
Zawarte są w niej ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych w urzędzie gminy leszno
Ponadto stanowi ona podstawę do opracowania instrukcji szczegółowych uwzględniających specyfikę poszczególnych systemów informatycznych.

2. **Definicje**

1) **Ustawa** – ustawa o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922);
2) **Rozporządzenie** – 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 systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 104, poz. 1024);
3) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
4) **Użytkownik systemu** – osoba, która przetwarza dane osobowe na podstawie upoważnienia Administratora Danych Osobowych posiadająca przyporządkowany jej identyfikator i hasło dostępu do pracy w systemie informatycznym;
5) **Administrator Danych Osobowych** – organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych,
6) **Informatyk** – osoba odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób nieupoważnionych do systemów oraz podejmowanie odpowiednich działań w przypadku stwierdzenia naruszeń w tych systemach.

3. **Bezpieczna eksploatacja sprzętu i oprogramowania**

1. Sprzęt służący do przetwarzania danych osobowych składa się z: komputerów stacjonarnych klasy PC, notebooków oraz serwerów.
2. Sieć komputerowa służąca do przetwarzania danych osobowych posiada zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
3. Główne węzły są podtrzymywane przez UPS zapewniający odpowiedni czas pracy systemu.
4. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
5. Informatyk odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.
6. Ekrany monitorów są wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.

7. Ekrany monitorów, są ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

4. **Procedura nadawania uprawnień do przetwarzania danych osobowych.**

1. Do przetwarzania danych osobowych w systemie informatycznym mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych.
2. Użytkownikom systemu, którzy przetwarzają dane osobowe w systemie informatycznym na podstawie upoważnienia, o którym mowa w ust. 1, przyznawane są indywidualne identyfikatory z hasłem inicjującym.
3. Informatyk na podstawie upoważnienia, o którym mowa w ust. 1, rejestruje użytkownika w systemie oraz nadaje mu identyfikator.
4. Identyfikator użytkownika wraz z jego imieniem i nazwiskiem, Informatyk przekazuje Administratorowi Danych Osobowych lub wyznaczonej przez niego osobie w celu wpisania do Ewidencji osób upoważnionych do przetwarzania danych osobowych.
5. Dostęp do danych osobowych przetwarzanych w systemie informatycznym jest możliwy wyłącznie po wpisaniu identyfikatora użytkownika oraz hasła.
6. Identyfikator użytkownika systemu stanowi ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
7. Hasło użytkownika systemu stanowi ciąg znaków literowych, cyfrowych lub innych, przypisane do identyfikatora użytkownika systemu, znane jedynie jemu.
8. W przypadku zmiany przez użytkownika uprawnień do obsługi danego systemu, kierownik komórki organizacyjnej występuje z wnioskiem do Informatyka o modyfikację uprawnień.
9. W przypadku utraty przez użytkownika uprawnień do obsługi danego systemu informatycznego (np. rozwiązanie stosunku pracy, nieobsługiwanie systemu z powodu zmiany stanowiska pracy) pracownik zajmujący się sprawami kadrowymi występuje do Informatyka o anulowanie upoważnienia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych.
10. Identyfikator użytkownika systemu nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
11. Informatyk posiada przydzielony przez Administratora Danych Osobowych w systemie informatycznym identyfikator użytkownika uprzywilejowanego.
12. Użytkownikom systemu zabrania się:
    - ujawniania własnego identyfikatora i hasła współpracownikom i osobom z zewnątrz,
    - udostępniania stanowisk pracy z danymi osobowymi osobom nieuprawnionym,
    - pozostawiania własnych haseł w miejscach, do których mogą mieć dostęp inne osoby,
    - korzystania z komputerów nie związanych z własnym stanowiskiem pracy,
    - udostępniania osobom nieuprawnionym jakichkolwiek informacji na temat programów komputerowych zainstalowanych w systemie.

5. **Metody i środki uwierzytelnienia.**

1. Pierwsze hasło dla użytkownika systemu przydziela Informatyk przy wprowadzaniu identyfikatora użytkownika do systemu.
2. Użytkownik systemu jest zobowiązany do natychmiastowej zmiany hasła inicjującego.
3. Informatyk wymusza zmianę haseł inicjujących wszystkich użytkowników systemu.
4. Hasło użytkownika systemu powinno mieć minimum 8 znaków i być zmieniane co 30 dni.
5. Hasło użytkownika systemu zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
6. Hasło wpisane z klawiatury komputera nie może pojawiać się na ekranie monitora w formie ujawnionej.
7. Za systematyczną, terminową zmianę hasła odpowiada użytkownik systemu.
8. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
9. W systemie, w którym nie następuje automatyczne wymuszanie zmiany hasła, hasło zmienia użytkownik systemu.
10. Użytkownik systemu niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez Informatyka.
11. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło dostępu.
12. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów itp.
13. Właścicielem hasła jest użytkownik systemu.
14. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
15. Osobą odpowiedzialną za przydział haseł, a także w zakresie rejestrowania i wyrejestrowania użytkowników jest Informatyk.
16. Za wszelkie operacje w systemie wykonywane z wykorzystaniem indywidualnego identyfikatora oraz hasła odpowiada właściciel identyfikatora.
17. W przypadku, gdy zaistnieje podejrzenie, że dane hasło poznała osoba nieuprawniona, użytkownik systemu zobowiązany jest do niezwłocznego powiadomienia o powyższym fakcie Administratora Danych Osobowych celem wszczęcia i zastosowania przewidzianych w takich sytuacjach procedur, a także do natychmiastowej zmiany hasła i powiadomienia Informatyka.

Hasła Informatyka.

1. Informatyk zobowiązany jest zmienić swoje hasło nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasła administratora wymienione powinny być spisane oraz umieszczane w zamkniętych kopertach, odrębnych dla każdego z systemów, w miejscu uniemożliwiającym dostęp do nich osób nieupoważnionych, chroniącym przed utratą lub zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także Administratorowi Danych Osobowych w przypadkach nadzwyczajnych.
3. Zarejestrowane hasła administratora, oprócz treści hasła winny posiadać adnotację o dacie ich wprowadzenia do systemu oraz być przechowywane przez okres 5 lat.

4. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

6. **Procedura rozpoczęcia, zawieszenia i zakończenia pracy.**

1. Rozpoczęcie pracy na komputerze przez użytkownika systemu następuje po poprawnym zalogowaniu się do systemu informatycznego (uwierzytelnieniu).
2. Rozpoczęcie pracy w aplikacji musi być prowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji, a w przypadku braku takiej w dokumentacji według zasad opracowanych przez Informatyka.
3. Jeśli system to umożliwia, po przekroczeniu 3 prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika systemu.
4. Informatyk ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Administratora Danych Osobowych.
5. Przed opuszczeniem stanowiska pracy, użytkownik systemu obowiązany jest:
   a) wylogować się z systemu informatycznego lub,
   b) wywołać blokowany hasłem wygaszacz ekranu.
6. Kontynuacja pracy po powrocie powinna być możliwa jedynie po ponownym uwierzytelnieniu (w przypadku wylogowania) lub odblokowaniu systemu komputerowego przez wprowadzenie hasła.
7. Zakończenie pracy w systemie informatycznym polega na przeprowadzeniu operacji wylogowania z systemu, a także poprzez uruchomienie odpowiedniej dla systemu wersji jego zamknięcia, w przypadku braku takiej w dokumentacji według zasad opracowanych przez Informatyka oraz po wyłączeniu systemu komputerowego.
8. Użytkownik systemu jest zobowiązany upewnić się, czy proces wylogowywania zakończył się pomyślnie.
9. Po zakończeniu pracy w systemie informatycznym użytkownik systemu jest zobowiązany zabezpieczyć stanowisko pracy, a w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.
10. W pomieszczeniach gdzie znajdują się stanowiska komputerowe absolutnie nie mogą samodzielnie przebywać osoby, które nie posiadają upoważnień do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w pomieszczeniach, w których są przetwarzane dane osobowe jest możliwe tylko na podstawie indywidualnego pozwolenia wydanego przez Administratora Danych Osobowych i tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
11. Każdy użytkownik systemu ma bezwzględny obowiązek wylogowania się z systemu w przypadku zaplanowanej dłuższej nieobecności na danym stanowisku komputerowym lub w przypadku wcześniejszego lub całkowitego zakończenia pracy.
12. Jakiekolwiek stanowisko komputerowe nie może pozostawać z uruchomionym i dostępnym systemem bez dozoru pracującego na nim użytkownika systemu.
13. Każdy użytkownik systemu w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe, używane narzędzia programowe, a także sprzętowe zobowiązany jest do natychmiastowego zaprzestania pracy i wyłączenia sprzętu.

14. Każdy użytkownik systemu niezwłocznie o faktach wymienionych w ust. 13 powiadamia Administratora Danych Osobowych, a także Informatyka.
15. Każdy użytkownik systemu niezwłocznie powiadamia Informatyka w przypadku braku możliwości zalogowania się na swoje konto, lub jakichkolwiek trudnościach i występujących przeszkodach w tym procesie.
16. Informatyk monitoruje rozpoczęcie i zakończenie pracy systemu informatycznego.
17. Informatyk ma prawo do monitorowania pracy urządzeń przyłączonych do sieci informatycznej w zakresie przesyłania i przetwarzania danych, rejestracji zdarzeń związanych z przesyłaniem i przetwarzaniem danych w oprogramowaniu oraz prawidłowości wykorzystania powierzonego użytkownikom systemu sprzętu i oprogramowania.
18. Informacje pozyskane w wyniku monitorowania działań użytkowników systemu oraz pracy urządzeń mogą zostać wykorzystane wyłącznie do celów służbowych, związanych z bezpieczeństwem przetwarzania danych osobowych w systemach informatycznych.

7. Procedura tworzenia kopii zapasowych.

1. Zbiory danych osobowych przetwarzanych w systemie informatycznym, są dodatkowo zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci;
   b) tworzenia kopii zapasowych w sposób określony ustawą i rozporządzeniem.
2. Za tworzenie kopii zapasowych systemu informatycznego odpowiedzialny jest Informatyk.
3. Kopie są wykonywane przy pomocy wbudowanych funkcji systemu.
4. Kopie zapasowe:
   a. sporządza się na dysk twardy komputera umieszczonego w innym pomieszczeniu niż system, zabezpieczony przed nieuprawnionym dostępem;
   b. przechowuje się przez minimum 1 miesiąc.
5. Każdorazowo przed aktualizacją lub jakąkolwiek zmianą w systemie należy wykonać pełną kopię zapasową systemu.
6. Kopie zapasowe należy okresowo sprawdzać w celu ich przydatności do odtworzenia w przypadku jakiejkolwiek awarii systemu, odpowiedzialny za wskazane czynności jest Informatyk.
7. Nośniki danych po ustaniu ich przydatności należy pozbawić danych i zniszczyć w sposób uniemożliwiający odczyt danych osobowych.

8. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji, kopii zapasowych i wydruków.

1. Wszelkie nośniki informatyczne, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieupoważnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
2. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, nośnik niszczy się trwale w sposób uniemożliwiający odczytanie danych.

3. Usuwanie danych z systemu musi być zrealizowane przy pomocy właściwego oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji. Za wskazany proces odpowiada Informatyk.
8. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie do stanu nie dającego możliwości odzyskania danych.
5. Decyzję o likwidacji danych osobowych przetwarzanych bezpośrednio w systemie informatycznym oraz danych osobowych przechowywanych w kopiach zapasowych podejmuje osoba nadzorująca pracę na określonym zbiorze danych osobowych w porozumieniu z Administratorem Danych Osobowych.
6. Dla udokumentowania likwidacji danych, o których mowa w ust. 5 likwidujący sporządza protokół zawierający niezbędne informacje o usuniętych danych.
7. Fakt niszczenia kopii zapasowych, Informatyk odnotowuje w rejestrze kopii zapasowych.
8. Przechowywane w systemie informatycznym, na kopiach zapasowych lub w postaci wydruków dane osobowe, które przestały być użyteczne, podlegają usunięciu lub zniszczeniu w sposób trwały uniemożliwiający ich odczytanie.
9. Kopie zapasowe przechowuje się przez okres określony dla poszczególnych danych osobowych zgodnie z ustalonymi przepisami.
10. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są wykonywane na płytach CD, DVD i są przechowywane w pomieszczeniach innych niż te, w których przechowuje się zbiory danych osobowych wykorzystywane do bieżących prac kancelaryjno-biurowych.
11. Wydruki oraz elektroniczne nośniki informacji z danymi osobowymi pochodzącymi z systemu informatycznego, które nie są przeznaczone do udostępniania, przechowuje się w zamykanych szafach i pomieszczeniach, do których dostęp mogą mieć wyłącznie uprawnieni użytkownicy systemu.
12. Zabrania się pozostawiania dokumentów, kopii dokumentów, wydruków z danymi osobowymi w drukarkach, kserokopiarkach itp.
13. Wydruki i dokumenty wykorzystane w pracach kancelaryjno-biurowych należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarkach dokumentów.
14. Pomieszczenia, w których przetwarzane są dane osobowe na czas nieobecności osób zatrudnionych należy zamykać, w sposób uniemożliwiający dostęp do nich osobom postronnym. Kategorycznie zabrania się pozostawiania kluczy w drzwiach, szafach, biurkach, a także pozostawiania otwartych lub nieprawidłowo zamkniętych drzwi pomieszczeń, w których przetwarzane są dane osobowe.

9. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

1. Komputery zainstalowane w sieci informatycznej posiadają zainstalowany firewall i program antywirusowy.
2. Program antywirusowy powinien być uaktywniony cały czas podczas pracy danego systemu.
3. Za ochronę antywirusową odpowiada Informatyk.
4. Wszystkie pliki otrzymywane z zewnętrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania wirusów najnowszą dostępną wersją

programu antywirusowego. Sprawdzenie odbywa się automatycznie przez system antywirusowy lub ręcznie przez użytkowników systemu.

5. Zabrania się użytkownikom systemu wyłączania, odinstalowywania programów zabezpieczających komputer (firewall, program antywirusowy).
6. W przypadku, gdy użytkownik systemu zauważy komunikat wskazujący na zaistnienie zagrożenia zobowiązany jest do natychmiastowego zaprzestania jakichkolwiek czynności w systemie.
7. W przypadku wskazanym w ust. 6 użytkownik systemu zobligowany jest do natychmiastowego powiadomienia Informatyka i Administratora Danych Osobowych.
8. Informatyk zobowiązany jest do dopilnowania, aby zainstalowany program antywirusowy był tak skonfigurowany, by dokonywał aktualizacji bazy wirusów, a także by było zagwarantowane automatyczne sprawdzanie każdego komputera pod kątem ewentualnej obecności wirusów komputerowych.
9. Osoby użytkujące komputer przenośny, dopuszczony do przetwarzania danych osobowych, zobowiązane są w szczególności do:

1) zachowania szczególnej ostrożności podczas transportu i przechowywania komputera;
2) stosowania odpowiedniego hasła do systemu;
3) szyfrowania danych prawnie chronionych,

w celu zapobieżenia dostępowi do danych osobowych osobom nieupoważnionym.

Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

1. Informatyk jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   a) sieci lokalnej i sieci rozległej (firewall na routerze),
   b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej (firewalle na komputerze).
2. Użytkownicy systemu obowiązani są do utrzymywania stałej aktywności zainstalowanego na ich stanowiskach komputerowych specjalistycznego oprogramowania monitorującego wymianę danych na styku tego stanowiska i sieci lokalnej.

10. **Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych**

1. System informatyczny powinien zapewniać odnotowanie informacji o odbiorcach, w rozumieniu art. 7 pkt 6 Ustawy, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia.
2. Nie stosuje się ust. 1 w przypadku, gdy system informatyczny używany jest do przetwarzania danych osobowych zawartych w zbiorach jawnych.
3. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w urzędzie gminy leszno,
   c) przedstawiciela, o którym mowa w art. 31a ustawy,
   d) podmiotu, któremu powierzono przetwarzanie danych,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

4. Dane osobowe administrowane przez urząd gminy leszno mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy ustawy oraz innych przepisów powszechnie obowiązujących.
5. Dane osobowe udostępnia się na pisemny wniosek, chyba, że przepis innej ustawy stanowi inaczej.
6. Dane udostępnione urzędowi gminy leszno przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

11. Procedura wykonywania przeglądów i konserwacji

1. Przeglądy i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu oraz zgodnie z harmonogramem Informatyka.
2. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada Informatyk. Sprawdzana jest m.in. spójność danych oraz stan nośników informacji.
4. Informatyk okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.
5. Nieprawidłowości w działaniach systemu informatycznego oraz oprogramowania powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.
6. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
7. W przypadku naprawy sprzętu komputerowego dane osobowe należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza terenem danej jednostki, po zabezpieczeniu - usunąć z dysku. Gdy nie ma możliwości usunięcia danych naprawa powinna być nadzorowana przez osobę upoważnioną przez administratora systemu.
8. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji może być dokonana tylko przy udziale Informatyka i za zgodą Administratora Danych Osobowych.

12. Zarządzanie oprogramowaniem

1. W urzędzie gminy Leszno zobowiązuje się wszystkich do używania jedynie legalnego oprogramowania.
2. Instalacje oprogramowania na stanowiskach pracowniczych mogą być dokonywane z nośników znajdujących się w zasobach urzędu gminy Leszno. Instalowanie oprogramowania nie będącego w zasobach urzędu gminy leszno ma być konsultowane z informatykiem. Instalacja i korzystanie z produktów w wersjach ewaluacyjnych, testowych lub w jakikolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane zgodnie z ich przeznaczeniem.

3. Za całość zagadnień związanych z instalowaniem, użytkowaniem oprogramowania w urzędzie gminy leszno jest odpowiedzialny Informatyk.
4. Oryginalne dokumenty licencyjne (karty rejestracyjne, narzędzia, nośniki etc.) dla używanego w urzędzie gminy leszno oprogramowania, przechowywane są przez Informatyka.

13. Postanowienie końcowe

1. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy Ustawy oraz wydanych na jej podstawie aktów wykonawczych.
2. Instrukcja wchodzi w życie z dniem podpisania.