WÓJT
GMINY WIENIAWA

Zarządzenie Nr 12.2018

Wójta Gminy Wieniawa z dnia 31 stycznia 2018 roku w sprawie: ochrony informacji prawnie chronionych przetwarzanych w Urzędzie Gminy Wieniawa

Na podstawie art. 33 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2013 r., poz. 594 z późn.zm.), art. 3, art. 36 ust.3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100, poz. 1024), ustawy z dnia 29 września 1994 roku o rachunkowości (Dz.U. z 2013 r., poz. 330 z późn.zm.) oraz ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz.1228 z późn. zm.)

zarządzam, co następuje:

§ 1.

1. Ilekroć dalej jest mowa o:

a) „urzędzie" – należy przez to rozumieć Urząd Gminy Wieniawa,

b) „wójcie" – należy przez to rozumieć Wójta Gminy Wieniawa,

c) „komórce organizacyjnej" - należy przez to rozumieć referat / samodzielne stanowisko w Urzędzie Gminy Wieniawa,

d) ABI – Administrator Bezpieczeństwa Informacji,

e) ADO – Administrator Danych Osobowych,

f) ASI – Administrator Systemu Informatycznego.

2. W urzędzie są przetwarzane dane, czyli zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane dane osobowe pracowników i innych osób mających interes prawny w urzędzie.

3. Dane osobowe przetwarza się wyłącznie dla określonych celów związanych z działalnością urzędu.

4. W przypadku tworzenia innych zbiorów danych osobowych, administrator danych osobowych rejestruje je zgodnie z przepisami rozdziału 6 ustawy o ochronie danych osobowych.

5. Przetwarzanie danych osobowych może odbywać się w systemie informatycznym, a także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

6. Informacje prawnie chronione na podstawie innych przepisów niż ustawa o ochronie danych osobowych, należy chronić realizując przepisy tych ustaw oraz wytyczne wynikające z niniejszego zarządzenia.

§ 2.

1. Administratorem danych osobowych - w urzędzie w rozumieniu ustawy o ochronie danych osobowych jest Wójt.

2. Wójt może ustanowić pełnomocnika ADO, Inspektora Danych Osobowych, który będzie sprawował nadzór nad realizacją niniejszego zarządzenia i realizował zadania ADO urzędu.

3. Zadania ADO określa ustawa o ochronie danych osobowych oraz przepisy wykonawcze.

§ 3.

1. W celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych w systemach informatycznych urzędu, powołuje się Inspektora Danych Osobowych, pełniącego rolę ABI

2. Zadania ABI określa Polityka bezpieczeństwa informacji w Urzędzie Gminy Wieniawa.

3. Zadania ABI, ADO może zlecić podmiotowi zewnętrznemu, na podstawie zawartej umowy.

§ 4.

1. W celu organizacji, administrowania, zabezpieczenia i kontroli systemów informatycznych ADO może powołać Administratora Systemu Informatycznego.

2. Do momentu powołania Administratora Systemu Informatycznego, obowiązki ASI urzędu pełnią Kierownicy Referatów w odniesieniu do pracowników, wobec których pełnią oni rolę bezpośredniego przełożonego.

3. Zadania ASI określa Polityka bezpieczeństwa informacji w Urzędzie Gminy Wieniawa.

4. Zadania ASI, ADO może zlecić podmiotowi zewnętrznemu, na podstawie zawartej umowy.

§ 5.

W zakresie przetwarzania informacji prawnie chronionych wprowadza się:

1. „Politykę bezpieczeństwa informacji w Urzędzie Gminy Wieniawa" – załącznik nr 1.

2. „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania informacji prawnie chronionej w tym danych osobowych Urzędzie Gminy Wieniawa" – załącznik nr 2.

§ 6.

1. Kierownicy komórek organizacyjnych urzędu są zobowiązani do nadzorowania zasad przetwarzania danych osobowych w podległych komórkach, zgodnie z kompetencjami.
2. Kierownicy komórek organizacyjnych urzędu są zobowiązani do bieżącego aktualizowania upoważnień podległych pracowników pod kątem ochrony danych, zgodnie z przydzielonymi zadaniami.
3. Do przetwarzania danych osobowych mogą być dopuszczeni wyłącznie pracownicy posiadający upoważnienie wydane przez ADO.
4. Przetwarzanie danych osobowych w systemach informatycznych może odbywać się tylko na programach dopuszczonych do użytkowania przez ADO.

§ 7.

1. Osoby, których dane są przetwarzane w urzędzie, mają prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualnienia lub poprawiania, jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.
2. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia ADO lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku czynności wykonywanych przez osoby działające z upoważnienia podmiotów uprawnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
3. Upoważnienie, o którym mowa w pkt.2, wynikać może w szczególności z:
a) charakteru pracy wykonywanej na danym stanowisku pracy lub
b) dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na danym stanowisku pracy lub
c) odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.
4. Osoby, które zostały upoważnione do przetwarzania danych osobowych, są zobowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia.
5. W zakresie przetwarzania danych osobowych w systemach innych niż informatyczne, obowiązują przepisy o tajemnicy służbowej, obiegu i zabezpieczeniu dokumentów służbowych.

§ 8.

1. Organizacja i funkcjonowanie ochrony informacji niejawnych określone są odrębnym zarządzeniem Wójta.
2. Zapewnienie przestrzegania przepisów o ochronie informacji niejawnych podlega Pełnomocnikowi Wójta do spraw ochrony informacji niejawnych.
3. Zakres działania i upoważnienia Pełnomocnika do ochrony informacji niejawnych określone są odrębną dokumentacją.
4. W zakresie przepisów ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych należy przestrzegać postanowień wynikających z „Planu ochrony informacji niejawnych w Urzędzie Gminy Wieniawa" oraz "Instrukcji ochrony informacji niejawnych Urzędu Gminy Wieniawa".
5. W urzędzie informacje niejawne nie są przetwarzane w systemach teleinformatycznych.

§ 9.

Zarządzenie wchodzi w życie z dniem podjęcia z mocą obowiązującą od dnia 01 marca 2018 r.

WÓJT GMINY WIENIAWA

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik Nr 1
do Zarządzenia Nr 12.2018
Wójta Gminy Wieniawa
z dnia 31 stycznia 2018 r.

Polityka Bezpieczeństwa Informacji
w Urzędzie Gminy Wieniawa

Wieniawa 2018

§ 1.

Część ogólna

1. Polityka bezpieczeństwa Informacji w Urzędzie Gminy Wieniawa – zwana dalej Polityką została opracowana na podstawie obowiązujących przepisów prawa:
   1. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024),
   2. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. Nr 922 z 2016r., z późniejszymi zmianami) oraz przepisów wykonawczych z nią związanych oraz innych przepisów, ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii,
   3. ustawy z dnia 29 września 1994r. o Rachunkowości (Dz. U. z 2017 r. poz. 2342 i 2201 z 2018 r. poz. 62)

oraz według zasad Systemu Zarządzania Bezpieczeństwem Informacji Norma Międzynarodowa ISO/IEC 27001:2005 Polska Norma PN-ISO/IEC 27001:2007.

2. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zestaw praw, reguł i zaleceń, regulujących sposób i zarządzania, ochrony i dystrybucji wewnątrz Urzędu Gminy Wieniawa.
3. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzania danych osobowych.
4. Niniejszą Politykę stosuję się do:
   1. danych osobowych:

   - przetwarzanych w systemach informatycznych,
   - zapisanych na zewnętrznych nośnikach informacji,
   - przetwarzanych tradycyjnie.

   2. Informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:

   - służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,
   - dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
5. Bez względu na zajmowane stanowisko w Urzędzie Gminy Wieniawa, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe.

§ 2.
Definicje

Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz wszystkich pozostałych dokumentów, które zostały przyjęte przez Urząd Gminy Wieniawa, w zakresie ochrony przetwarzania danych:

1. **Administrator Danych Osobowych –ADO** - Wójt Gminy Wieniawa
2. **Administrator Bezpieczeństwa Informacji – ABI** – osoba wyznaczona przez ADO.
3. **Administrator Systemów Informatycznych – ASI** – osoba wyznaczona przez ADO.
4. **Bezpieczeństwo przetwarzania danych osobowych** – zachowanie poufności, integralności i rozliczalności danych osobowych; dodatkowo mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
5. **Dane osobowe** – każda informacja dotycząca żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikację osoby.
6. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.
7. **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
8. **Naruszenie danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie ochrony danych osobowych.
9. **Poufność** – właściwość zapewniająca, że informacja jest dostępna jedynie osobom upoważnionym.
10. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
11. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

12. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

13. **Urząd** – Urząd Gminy Wieniawa.

14. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.

15. **Użytkownik zewnętrzny** – osoba nie będąca pracownikiem lub stażystą Urzędu Gminy Wieniawa, posiadająca uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na rzecz urzędu.

16. **Właściciel zbioru danych osobowych** – osoba kierująca komórką organizacyjną, stanowisko samodzielne, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce organizacyjnej lub na stanowisku samodzielnym. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

17. **Zbiór danych osobowych** – każdy posiadający uporządkowaną strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

18. **Zbiór nieinformatyczny** – każdy posiadający uporządkowaną strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

19. **Sieć lokalna** – połączenie funkcjonujących w Urzędzie Gminy Wieniawa systemów informatycznych i stacji roboczych przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

20. **Stacja robocza** - stacjonarny lub przenośny komputer, rozpoznawany przez system IT, wchodzący w skład systemu informatycznego, umożliwiający użytkownikom dostęp do danych znajdujących się w tym systemie.

21. **Sieć telekomunikacyjna** – sieć telekomunikacyjna w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz. 1800, z późniejszymi zmianami).

§ 3.

Wprowadzenie niniejszej Polityki ma na celu określenie jednolitych zasady dla całego systemu przetwarzania danych.

Procesy i procedury podlegające wdrożeniu to:

1) ochrona przetwarzanych i gromadzonych informacji, w tym danych osobowych w urzędzie i dotyczy:
   a) zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,
   b) metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,
   c) procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,
   d) ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,
   e) określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny,
2) oszacowanie i zmniejszenie ryzyka utraty informacji,
3) określenia zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych w tym danych osobowych,
4) podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych informacji.

Powyższe procedury systemu teleinformatycznego, odnoszą się w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,

2) informacji będących własnością Urzędu Gminy Wieniawa lub jednostek organizacyjnych gminy, o ile zostały przekazane do urzędu na podstawie umów lub porozumień,

3) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,

4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,

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

§ 4.
Uprawnienia do przetwarzania danych

1. Dostęp do systemu informatycznego, programów przetwarzających dane osobowe oraz urządzeń z nimi powiązanych możliwy jest wyłącznie na podstawie upoważnienia wydanego przez ADO.

2. Przed dopuszczeniem do pracy w systemie informatycznym, każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą Polityką.

3. Użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia.

4. W celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych w systemach informatycznych urzędu, ADO powołuje **administratora bezpieczeństwa informacji.**

5. W celu prawidłowego funkcjonowania infrastruktury informatycznej (sprzęt, systemy i aplikacje informatyczne) ADO powołuje **administratora systemów informatycznych.**

§ 5.
Zakres działania ABI

1. ABI w zakresie swojego działania w urzędzie podlega bezpośrednio ADO lub pełnomocnikowi ADO lub osobie przez niego upoważnionej.
2. ABI sprawuje nadzór nad kierownikami komórek organizacyjnych urzędu w zakresie przetwarzania danych osobowych w ich komórkach.
3. ABI prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych.

4. ABI prowadzi elektroniczny wykaz baz danych w systemach informatycznych, w których przetwarzane są informacje prawnie chronione – dane osobowe.
5. Do zakresu działania ABI należy również:

- nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób,
- zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
- dopilnowanie aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby komputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych,
- nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
- zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które zawarte są w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
- nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania w przypadku awarii systemu,
- nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
- nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
- nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny,
- nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych,
- podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniach zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,

- analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie ADO odpowiednich zmian do Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych,
- koordynacja procesu analizy i oceny ryzyka związanego z przetwarzaniem danych osobowych z uwzględnieniem zabezpieczenia systemu informatycznego w urzędzie w tym: proponowanie ADO mechanizmów ochrony i środków bezpieczeństwa przetwarzania danych osobowych,
- ścisła współpraca ze służbami prawnymi i wyznaczonymi pracownikami urzędami w prawnych aspektów procesu przetwarzania danych osobowych,
- koordynacja wprowadzania poziomów bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym,
- określanie i nadzór nad wdrażaniem standardów zabezpieczeń,
- opiniowanie wszelkich zmian zachodzących w procesie przetwarzania danych osobowych, pod kątem ich wpływu na bezpieczeństwo,
- niezwłoczne reagowanie na incydenty w zakresie bezpieczeństwa systemu informatycznego, informowanie ADO o incydentach, skutkach i propozycjach konsekwencji służbowych dla pracowników,
- nadzór nad przestrzeganiem przez pracowników zasad ochrony danych osobowych obowiązujących w urzędzie,
- monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym i dopasowanie systemu do wymagań prawnych,
- koordynacja bieżących działań związanych ze szkoleniami pracowników, informowaniem pracowników o zagrożeniach,
- opracowanie i aktualizowanie „Polityki bezpieczeństwa informacji w Urzędzie Gminy Wieniawa" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania informacji prawnie chronionych, w tym danych osobowych w Urzędzie Gminy Wieniawa" zgodnie z rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
- monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym i dopasowanie systemu do wymagań prawnych,
- rejestracja zbiorów danych osobowych w ogólnopolskim rejestrze zbiorów danych prowadzonych przez GIODO i aktualizacja danych w rejestrze,

- monitorowanie zaleceń i interpretacji GIODO w zakresie ochrony danych osobowych i implementowanie ich w urzędzie,
- ABI reprezentuje ADO w obszarach związanych z nadzorowaniem przestrzegania obowiązujących zasad bezpieczeństwa danych osobowych oraz koordynuje procesy związane z zarządzaniem systemem informatycznym, przetwarzają cym dane osobowe w aspekcie ich bezpieczeństwa,
- nadzorowanie wewnętrznego audytu bezpieczeństwa systemu w porozumieniu z ADO.

§ 6.

Zakres działania ASI

1. Zarządzanie i administrowanie bazami danych.
2. Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
3. Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z obowiązującymi przepisami, Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Wieniawa.
4. Zarządzanie i administrowanie serwerami aplikacyjnymi: konfigurowanie, optymalizacja, monitorowanie, analizowanie zdarzeń systemowych, lokalizowanie błędów, diagnostyka i ich usuwanie.
5. Kontrola i wdrażanie polityki bezpieczeństwa na serwerach.
6. Implementacja odpowiednich mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej.
7. Techniczne nadawanie i odbieranie uprawnień zgodnie z przydzielonymi upoważnieniami, w porozumieniu z ABI.
8. Tworzenie kopii zapasowych zgodnie z Instrukcją zarządzania systemem informatycznym służącym do przetwarzania informacji prawnie chronionych, w tym danych osobowych w Urzędzie Gminy Wieniawa.
9. Bieżące monitorowanie poziomu bezpieczeństwa w systemie informatycznym, w szczególności bieżącego stanu aktualizacji systemów operacyjnych i serwerów oraz sygnatur programów antywirusowych.
10. Bieżące monitorowanie systemu informatycznego i systemu monitoringu wizyjnego urzędu i przekazywanie informacji o zagrożeniach ABI, a w przypadku jego nieobecności ADO.
11. Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz usuwanie ich skutków.
12. Zarządzanie określonymi rozwiązaniami technicznymi związanymi z ochroną systemu informatycznego.

13. Cykliczne przeglądy i weryfikacja :

- pomieszczeń dopuszczonych do przetwarzania danych,
- rozmieszczenia stacji roboczych,
- sprawności użytkowanego sprzętu, w tym konserwację i likwidację sprzętu i oprogramowania,
- legalności zainstalowanego oprogramowania,
- harmonogramu logowania do systemu informatycznego dla poszczególnych użytkowników,
- systemu informatycznego pod kątem obecności nieuprawnionego i szkodliwego oprogramowania,

14. Monitorowanie działania instalacji nagrywania rozmów telefonicznych i zabezpieczenie systemu przed niepowołanym odsłuchem.
15. Cykliczna kontrola sprawności zasilania awaryjnego infrastruktury telekomunikacji i sieci PC.
16. Przeprowadzanie szkoleń dla pracowników, w tym szczególnie dla nowo przyjętych.
17. Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacja umów z firmami świadczącymi usługi pogwarancyjne sprzętu komputerowego.
18. Prowadzenie bieżącej ewidencji licencji oprogramowania.
19. Przygotowywanie niezbędnej dokumentacji związanej z prawidłowym funkcjonowaniem sieci informatycznej (w tym: opisy systemów IT i zasilania).
20. Uczestnictwo w pracach projektowych i wdrożeniowych nowych rozwiązań.

§ 7.

Zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych

1. O naruszeniu ochrony danych osobowych mogą świadczyć symptomy występujące w następujących obszarach:
   1) w obrębie pomieszczeń, szaf lub miejsc przechowywania:
      a) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych , w szczególności do serwerowni oraz kas, gdzie przechowuje są nośniki kopii zapasowych,
      b) włamanie lub próby włamania do szaf, w których przechowywane są w postaci elektronicznej lub papierowej , nośniki danych osobowych,
   2) w obrębie sprzętu informatycznego:
      a) kradzież komputera, w którym przechowywane są dane osobowe,
      b) rozkręcona obudowa komputera,
   3) w obrębie systemu informatycznego i aplikacji:
      a) brak możliwości uruchomienia aplikacji pozwalającej na dostęp do danych osobowych,
      b) brak możliwości zalogowania się do tej aplikacji,

c) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w strukturze aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych),

d) poszerzone uprawnienia w obrębie aplikacji w stosunku do dotychczas przyznanych (na przykład wgląd do szerszego zakresu danych o pracownikach),

e) inny zakres lub różnice w zawartości zbioru danych osobowych dostępnych dla użytkownika (np. ich całkowity lub częściowy brak lub nadmiar),

Inne:

f) zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, pendrive'a itp.),

g) zagubienie bądź kradzież nośnika z zawartością danych osobowych,

2. Każda osoba, która zauważyła niepokojące zdarzenie, wystąpienie powyżej wymienionych symptomów lub innych objawów, które jej zdaniem mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania: bezpośredniego przełożonego, ASI, ABI lub ADO.
3. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż ADO, jest ona zobowiązana poinformować o tym fakcie ADO.
4. Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w urzędzie naruszenia bezpieczeństwa danych osobowych, ABI we współpracy z ASI, jest zobowiązany do podjęcia następujących kroków:

1) stwierdzenia czy rzeczywiście doszło do naruszenia ochrony danych osobowych, w tym:

a) sprawdzenia okoliczności zdarzenia,

b) wyjaśnienia jego przyczyn, w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,

2) w przypadku, gdy doszło do naruszenia ochrony danych osobowych to:

a) zebranie ewentualnych dowodów,

b) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,

c) zabezpieczenia danych przetwarzanych w systemie informatycznym, jego logów systemowych, logów programu i bazy w których nastąpiło naruszenie bezpieczeństwa oraz danych konfiguracyjnych całego systemu w celu późniejszej analizy

d) usunięcia skutków incydentu i przywrócenia pierwotnego stanu systemu informatycznego tj. stanu sprzed incydentu, polegające na:

- przeprowadzeniu analizy spójności danych osobowych przetwarzanych w systemie,
- ewentualnym odtworzeniu kopii zapasowych danych i plików konfiguracyjnych,
- przeprowadzeniu analizy poprawności funkcjonowania systemu informatycznego,
- powtórnym zabezpieczeniu danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.

5. System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

6. ABI określa, na podstawie zebranych informacji, przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym urzędu.

7. ABI prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

1) imię i nazwisko osoby zgłaszającej incydent,

2) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,

3) datę zgłoszenia incydentu,

4) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,

5) wyniki przeprowadzonych działań,

6) podjęte akcje naprawcze i ich skuteczność.

8. ABI odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

1) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,

2) określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,

3) określenia potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

§ 8.

Obszary przetwarzania informacji prawnie chronionych, w tym danych osobowych

1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi **załącznik nr 1 do niniejszej Polityki.**

2. Wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do przetwarzania danych stanowi **załącznik nr 2 do niniejszej Polityki.**

3. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi stanowi **załącznik nr 3 do niniejszej Polityki.**

4. W szczególnie uzasadnionych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych) wyłącznie za zgodą ADO i na zasadach określonych przez ABI.

5. W zakresie przetwarzania danych osobowych w systemach finansowo-księgowych, stosuje się również Politykę Rachunkowości oraz Instrukcję kasową.

§ 9.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje stu procentowego bezpieczeństwa danych, konieczne jest, aby każdy użytkownik mający styczność z przetwarzanymi danymi, świadomy odpowiedzialności, postępował zgodnie z przyjętymi w niniejszym dokumencie zasadami i minimalizował zagrożenie wynikające z błędów ludzkich.

2. Ochrona danych osobowych przetwarzanych w urzędzie obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w Urzędzie Gminy Wieniawa, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.

3. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.

4. Przetwarzać dane osobowe w systemach informatycznych jak i tradycyjnych zbiorach papierowych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych otrzymane od ADO.

5. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

6. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

7. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

8. Zachowanie tajemnicy służbowej obowiązuje pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

9. ABI i ADO jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w całym systemie urzędu.

10. **Techniczne środki zabezpieczające:**

- monitoring wizyjny w obrębie budynku urzędu, lokalizacja: Wieniawa ul. Kochanowskiego 88,
- zamki magnetyczne w serwerowni urzędu, system kontroli dostępu
- pełne drzwi do pomieszczeń biurowych z zamkiem typu YETI,
- szyby o podwyższonej odporności w pomieszczeniach zlokalizowanych na parterze,
- kasy pancerne lub szafy do dokumentów kadrowo-płacowych i backup danych i aplikacji IT,
- atestowane gaśnice przeciwpożarowe w pomieszczeniach biurowych,
- dedykowana sieć zasilania elektrycznego w lokalizacji ul. Kochanowskiego 88 dla serwerów oraz urządzeń klasy UPS na wypadek zaniku/braku zasilania elektrycznego w serwerowni urzędu,

- ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych

11. **Informatyczne środki zabezpieczające:**

- identyfikacja użytkownika komputera dopuszczonego do pracy, system informatyczny żąda podania loginu i hasła. Login i hasło wprowadzane jest indywidualnie użytkownikowi komputera przez ASI,
- wyposażenie stacji roboczych w mechanizm „wygaszacza ekranu" z wymuszoną procedurą ponownego logowania do stacji roboczej,
- identyfikacja użytkownika systemu dziedzinowego przy pomocy hasła i loginu,
- uprawnienia użytkownika systemu dziedzinowego nadawane przez ABI,
- mechanizm rejestracji czynności wykonywanych w systemie dziedzinowym przez użytkownika,
- przetwarzanie informacji na bazach danych wyłącznie w pomieszczeniu serwerowni,
- licencjonowane programy antywirusowe, automatyczna aktualizacja baz wirusów,
- systemowy nadzór nad ilością i jakością przetwarzanych danych,
- firewall na routerze lub UTM,
- system wykrywający obecność wirusów na poczcie elektronicznej,
- stosowanie ochrony newralgicznych elementów sieciowych – switche,
- program monitorujący przepływ informacji pomiędzy stanowiskami PC,
- program tworzący kopię danych
- filtracja treści internetowych poprzez UTM,
- zdalne monitorowanie zainstalowanego oprogramowania na komputerach użytkowników przez ASI
- automatyczne monitorowanie obciążenia sieci informatycznej na poszczególnych komputerach.

12. **Organizacyjne środki zabezpieczające:**

- indywidualne upoważnienia do dysponowania kluczami do pomieszczeń i budynków,
- indywidualne kody dostępu do serwerowni

- indywidualne hasła i loginy do systemów operacyjnych PC,
- indywidualne hasła i loginy do systemów dziedzinowych,
- uprawnienia wynikające z zakresu obowiązków i imiennych upoważnień,
- obowiązek otrzymania zgody na pracę w godzinach nadliczbowych lub w dni wolne,
- obowiązek zapoznania się z Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym,
- obowiązek nadzoru nad pracownikami przez bezpośrednich przełożonych,
- obowiązek udziału w szkoleniach z zakresu bezpieczeństwa przetwarzania danych.
- dokumentacja urzędu w zakresie ochrony danych osobowych,
- obowiązkowe szkolenia pracowników.

§ 10.

Sposób postępowania w zakresie komunikacji poza siecią informatyczną urzędu

1. Przy przesyłaniu danych osobowych poza siecią dedykowaną do transferu danych osobowych wymagane jest zastosowanie szczególnych wymagań w zakresie bezpieczeństwa. Obejmują one:

1) Zatwierdzenia w formie pisemnej lub w formie elektronicznej przez ADO celu wysłania danych osobowych,

2) Zastosowanie mechanizmów szyfrowania danych osobowych,

2. W przypadku stosowania mechanizmów kryptograficznych ADO określa wymagania w zakresie materiału kryptograficznego stosowanego do ochrony danych osobowych.

3. W wypadku, gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe, korzysta z innych mechanizmów kryptograficznych niż stosowane w Urzędzie Gminy Wieniawa, możliwe jest zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych. W tym celu ASI lub osoba specjalnie do tego celu wyznaczona, może przeprowadzić analizę poziomu bezpieczeństwa mechanizmu kryptograficznego oraz zgodności tego mechanizmu z komponentami systemu informatycznego.

4. W przypadku wystąpienia podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce, ABI zobowiązany jest poinformować o tym fakcie ADO i zmienić parametry klucza szyfrującego.

§ 11.

Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe poza siedzibą urzędu

1. Przetwarzanie danych osobowych na komputerach przenośnych poza siedzibą Urzędu Gminy Wieniawa, powinno być ograniczone do niezbędnego minimum i może się odbywać wyłącznie na podstawie umowy z ADO.

2. Umowa, o której mowa w ust.1 określa zasady korzystania z komputerów przenośnych, czas korzystania oraz wskazanie zakresu danych osobowych, których nie wolno przetwarzać na komputerze przenośnym.

3. Każdy komputer przenośny musi być zabezpieczony indywidualnym hasłem i loginem.

4. Pracownik korzystający z komputera przenośnego do przetwarzania danych osobowych lub dokumentów stanowiących tajemnicę służbową, zwłaszcza mających charakter lokalnej bazy lub pliku czyli zlokalizowanych bezpośrednio na użytkowanym komputerze, zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. W związku z powyższym użytkownik komputera przenośnego zobowiązany jest do:

   1) przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej 8 –mio znakowym zawierającym : duże i małe litery, znaki specjalne lub cyfry,

   2) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:

      a) transportowania komputera w odpowiedniej, przeznaczonej do tego celu torbie jako bagażu podręcznego,

      b) nie pozostawiania komputera w samochodzie, przechowalni bagażu, środkach transportu publicznego itp,

   3) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,

   4) zdecydowanego uniemożliwienia korzystania z komputera osobom niepowołanym (np. rodzinie, dzieciom, znajomym),

5) zabezpieczenia komputera przenośnego hasłem i utrzymanie konfiguracji oprogramowania systemowego w stanie wymuszającym korzystanie z tego hasła,

6) wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,

7) zmianę haseł co 30 dni,

8) blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,

9) regularnego i częstego kopiowania danych przetwarzanych na komputerze przenośnym, do systemu informatycznego Urzędu Gminy Wieniawa w celu umożliwienia wykonania kopii awaryjnej,

10) cyklicznego podłączania komputera do sieci informatycznej Urzędu Gminy Wieniawa w celu wykonania aktualizacji wzorców wirusów w programie antywirusowym,

5. ASI zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności:

1) dokonać konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł odpowiedniej jakości oraz ich cyklicznej zmiany, zgodnie z wytycznymi dotyczącymi polityki posługiwania się hasłami w systemie informatycznym Urzędu Gminy Wieniawa,

2) w przypadku przetwarzania danych osobowych znajdujących się bezpośrednio na komputerze przenośnym - zabezpieczyć je dodatkowo poprzez wykorzystanie oprogramowania szyfrującego

3) dokonać instalacji i konfiguracji oprogramowania antywirusowego,

4) przeprowadzić aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

6 ASI jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych poza siedzibą Urzędu Gminy Wieniawa. W szczególności ewidencja powinna obejmować:

1) typ i numer seryjny komputera przenośnego,

2) imię i nazwisko osoby będącej użytkownikiem komputera,

3) wykaz oprogramowania zainstalowanego na komputerze, służącego do przetwarzania danych osobowych

4) rodzaj i zakres danych osobowych przetwarzanych na komputerze.

7 W razie zgubienia lub kradzieży komputera przenośnego, pracownik zobowiązany jest do natychmiastowego powiadomienia ABI lub osoby uprawnionej zgodnie z zasadami informowania w przypadku naruszenia ochrony danych osobowych.

8 Kopie informacji przetwarzanych na komputerze przenośnym tworzone są indywidualnie przez ich użytkowników, na ich odpowiedzialność.

§ 12.

Elektroniczne zewnętrzne nośniki danych

1. W urzędzie stosuje się wyłącznie elektroniczne zewnętrzne nośniki danych (oznaczone i zarejestrowane przez ASI) oraz CD-ROM.
2. Nośniki pochodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu ich zawartości po uprzednim sprawdzeniu licencjonowanym programem antywirusowym w obecności ABI lub ASI.
3. Każdy użytkownik ma obowiązek usunięcia danych osobowych z nośników, które przeznaczone są do przekazania innemu podmiotów informacji związanych z realizacją zadań.
4. Deszyfracja i wprowadzenie do systemu informatycznego danych z nośników zewnętrznych dokonywana jest wyłącznie przez ABI.

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik Nr 1
do Polityki Bezpieczeństwa
Informacji
w Urzędzie Gminy Wieniawa

1. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza się budynki, pomieszczenia i części pomieszczeń, tworzące obszary, w których przetwarzane są dane osobowe.
2. Pod szczególną ochroną przed niepowołanym dostępem do danych osobowych pozostają urządzenia wchodzące w skład systemu informatycznego urzędu. W szczególności stacje robocze (poszczególne komputery), które powinny być umiejscawiane w sposób uniemożliwiający osobom nieuprawnionym, bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń służących do przetwarzania, a zwłaszcza kopiowania danych.
3. W budynku zlokalizowanym przy ul. Kochanowskiego 88 w Wieniawie na podstawie zawartej umowy o powierzeniu przetwarzania danych osobowych oraz informacji podlegających ochronie prawnej, która obejmuje:

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Lp.	Adres - budynek	Nr pomieszczeń
1.	**ul. Kochanowskiego 88, 26-432 Wieniawa**	**parter - 1,2**
2.	**ul. Kochanowskiego 88, 26-432 Wieniawa**	**I piętro - 3,4,5,6,7,8,9,10,11,12**
3.	**ul. Kochanowskiego 88, 26-432 Wieniawa**	**II piętro - 14,15,16,18,20**

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik Nr 2
do Polityki Bezpieczeństwa
Informacji
w Urzędzie Gminy Wieniawa

Wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do przetwarzania danych

Lp.	Nazwa zbioru	Sposób gromadzenia	Nazwa programu
1.	KADRY	Forma papierowa/ forma elektroniczna	Wolter Kluwer SA KADRY
2.	Płace	Forma papierowa/ forma elektroniczna	Wolter Kluwer SA PŁACE
3.	Elektroniczne Przelewy Bankowe	Forma elektroniczna	Centrum Usług Informatycznych CUI BS
4.	Płatnik	Forma papierowa/ forma elektroniczna	PŁATNIK
5.	Elektroniczne Zarządzanie Dokumentacją	Forma papierowa/ forma elektroniczna	EZD SIDAS
6.	Ewidencja wydanych zaświadczeń	Forma papierowa/ forma elektroniczna	Microsoft Word
7.	Ewidencja radnych i sołtysów	Forma papierowa/ forma elektroniczna	Microsoft Word
8.	Rejestr umów	Forma papierowa	Nie dotyczy
9.	Rejestr skarg i wniosków	Forma papierowa	Nie dotyczy
10.	Rejestr wniosków o udostępnienie informacji publicznej	Forma papierowa/ forma elektroniczna	Microsoft Word
11.	Kandydaci na ławników sądowych	Forma papierowa	Nie dotyczy
12.	Oświadczenia majątkowe	Forma papierowa	Nie dotyczy
13.	Rejestr Gospodarki Odpadami	Forma papierowa/ forma elektroniczna	Macrologic ERP
14.	Rejestr faktur i rachunków	Forma papierowa/ forma elektroniczna	Macrologic ERP
15.	Ewidencja wniosków i umów o zaopatrzenie w wodę i odprowadzanie ścieków	Forma papierowa/ forma elektroniczna	Microsoft Word
16.	Rejestr skazanych	Forma papierowa/ forma elektroniczna	Microsoft Word
17.	Windykacja należności cywilnoprawnych	Forma papierowa/ forma elektroniczna	Macrologic ERP
18.	Podatki i opłaty lokalne	Forma papierowa/	Macrologic ERP

		forma elektroniczna	
19.	System Informacji Oświatowej	Forma papierowa/ forma elektroniczna	SIO, Microsoft Word, Microsoft Excel
20.	Zamówienia publiczne	Forma papierowa/ forma elektroniczna	UZP Microsoft Word, Microsoft Excel
21.	Dofinansowanie prawodawcom kosztów kształcenia zawodowego młodocianych pracowników	Forma papierowa/ forma elektroniczna	Microsoft Word
22.	Informacje o wyrobach zawierających azbest	Forma papierowa/ forma elektroniczna	Microsoft Word
23.	Wykaz partnerów Wieniawskiego Klastra Energii	Forma papierowa	Microsoft Word
24.	Decyzje o warunkach zabudowy oraz o ustaleniu celu publicznego	Forma papierowa/ forma elektroniczna	Microsoft Word
25.	Decyzje środowiskowe	Forma papierowa/ forma elektroniczna	Microsoft Word
26.	Przyłącza wodociągowe i kanalizacyjne	Forma papierowa	Nie dotyczy
27.	Świadczenia Rodzinne	Forma papierowa Forma elektroniczna	Oprogramowanie do obsługi Świadczeń Rodzinnych (SR) Sygnity S.A/ CUI Bank Spółdzielczy
28.	Fundusz i Zaliczka Alimentacyjna/ Dłużnicy alimentacyjni	Forma papierowa Forma elektroniczna	Oprogramowanie do obsługi Funduszu Alimentacyjnego (FA) Sygnity S.A/ CUI Bank Spółdzielczy
29.	Zasiłek Dla Opiekuna	Forma papierowa Forma elektroniczna	Oprogramowanie do obsługi Świadczeń Rodzinnych (SR) Sygnity S.A/ CUI Bank Spółdzielczy
30.	„ Za życiem"	Forma papierowa Forma elektroniczna	Oprogramowanie do obsługi Świadczeń Rodzinnych (SR) Sygnity S.A/ CUI Bank

			Spółdzielczy
31.	Świadczenie wychowawcze	Forma papierowa Forma elektroniczna	Oprogramowanie do obsługi Świadczenia Wychowawczego (SW) Sygnity S.A/ CUI Bank Spółdzielczy
32.	Karta Dużej Rodziny	Forma papierowa Forma elektroniczna	SI KDR
33.	**USC** Akta i Księgi Stanu Cywilnego, Orzekanie w sprawach zmian imion i nazwisk, Protokoły i zaświadczenia, Rejestr testamentów, PESEL, Projekty aktów i wzmianek, migracja aktów stanu cywilnego	Forma papierowa Forma elektroniczna	ŹRÓDŁO, SELWIN z modułem RWWiN, TECHNIKA
34.	**EL** Rejestr mieszkańców, rejestr wyborców, rejestr cudzoziemców, spisy i statystyki, subskrypcje PESEL	Forma papierowa Forma elektroniczna	ŹRÓDŁO, SELWIN z modułem RWWiN, TECHNIKA
35.	**RDO** - Rejestr dowodów osobistych	Forma papierowa Forma elektroniczna	ŹRÓDŁO
36.	Kwalifikacja wojskowa	Forma papierowa/ forma elektroniczna	Microsoft Word
37.	Obrona Cywilna, Zarządzanie kryzysowe i sprawy obronne	Forma papierowa/ forma elektroniczna	Microsoft Word
38.	Archiwum zakładowe	Forma papierowa	Nie dotyczy
39.	Zezwolenia na sprzedaż napojów alkoholowych	Forma papierowa/ forma elektroniczna	CEIDG
40.	Ewidencja działalności gospodarczej	Forma papierowa/ forma elektroniczna	CEIDG
41.	Zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	Forma papierowa/ forma elektroniczna	Macrologic ERP
42.	Ewidencja przydomowych oczyszczalni ścieków i zbiorników bezodpływowych	Forma papierowa/ forma elektroniczna	Microsoft Word
43.	Ewidencja mienia komunalnego	Forma papierowa	Nie dotyczy

44.	Gospodarka nieruchomościami	Forma papierowa	Nie dotyczy
45.	Zarządzanie drogami	Forma papierowa	Nie dotyczy
46.	Rejestr nieruchomości stanowiących własność gminy	Forma papierowa	Nie dotyczy
47.	Szkody rolnicze	Forma papierowa/ forma elektroniczna	Microsoft Excel
48.	Zbiór najemców lokali użytkowych i mieszkalnych	Forma papierowa	Nie dotyczy
49.	Zbiór nabywców nieruchomości	Forma papierowa	Nie dotyczy
50.	Rejestr wniosków i zgłoszeń na wycinkę drzew	Forma papierowa	Nie dotyczy
51.	Wypis/wyrys z planu zagospodarowania przestrzennego oraz studium kierunków i zagospodarowania przestrzennego	Forma papierowa	Nie dotyczy
52.	Rozgraniczenie i podział nieruchomości	Forma papierowa/ forma elektroniczna	Microsoft Word
53.	Ochrona środowiska	Forma papierowa/ forma elektroniczna	Microsoft Word
54.	Planowanie przestrzenne	Forma papierowa/ forma elektroniczna	Microsoft Word
55.	Rejestr dowodów księgowych	Forma papierowa/ forma elektroniczna	Macrologic ERP
56.	Rejestr VAT	Forma papierowa/ forma elektroniczna	Macrologic ERP
57.	Wspólnoty gruntowe	Forma papierowa Forma elektroniczna	Microsoft Word

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik Nr 3
do Polityki Bezpieczeństwa
Informacji
w Urzędzie Gminy Wieniawa

Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi.

Lp.	Nazwa zbioru	Opis zbioru	Nr pokoju
1.	KADRY	nazwisko; pierwsze imię; drugie imię; nr akt; imię ojca; imię matki; nazwisko rodowe pracownika, nazwisko rodowa matki; data urodzenia; miejsce urodzenia; płeć; obywatelstwo; wykształcenie; ostatnio ukończona szkoła; rok ukończenia szkoły; zawód wyuczony; specjalność; znajomość języków; szczególna umiejętność; adres zamieszkania/zameldowania; seria i nr dowodu osobistego; data wydania; przez kogo wydany; PESEL; NIP; kod tyt. Ubezpieczenia; NFZ; nazwa banku; nr konta, numer telefonu, stopień niepełnosprawności,	9,14
2.	Płace	Nazwisko, imię, PESEL, data i miejsce urodzenia, imiona rodziców, adres zamieszkania lub pobytu, data zatrudnienia/zakończenia, nazwa banku, nr konta bankowego, skł. płac	9
3.	Elektroniczne Przelewy Bankowe	Nazwisko, imię, adres zamieszkania, nazwa banku, nr rachunku bankowego.	2,4,7,9,14,15
4.	Płatnik	Nazwisko, imię, stopień niepełnosprawności, PESEL, NIP, rodzaj dokumentu, seria i nr dokumentu, data ur., status ubezpieczonego, obywatelstwo, kod oddziału NFZ, Nazwa Oddziału NFZ, płeć, członkowie rodziny, kod stopnia pokrewieństwa, Obywatelstwo	9
5.	Elektroniczne Zarządzanie Dokumentacją	Imię, nazwisko, nazwa, adres zamieszkania lub pobytu, numer telefonu	3,4,5,6,7,9,10,12, 14,15,16,20
6.	Ewidencja wydanych zaświadczeń	Imię i nazwisko, adres zamieszkania, data zatrudnienia, skł wynagrodzenia, PESEL,	3,4,5,6,9,10,16,20
7.	Ewidencja radnych i sołtysów	Imię, nazwisko, adres zamieszkania lub pobytu, numer telefonu, NIP,	14

		PESEL	
8.	Rejestr umów	strony umowy: imię i nazwisko, nazwa, adres zamieszkania lub pobytu , przedmiot umowy, kwota wynagrodzenia, nr konta bankowego, PESEL, adres e-mail,	16
9.	Rejestr skarg i wniosków	nazwa, imię i nazwisko, adres zamieszkania lub pobytu, nr telefonu, adres e-mail,	14
10.	Rejestr wniosków o udostępnienie informacji publicznej	nazwa, imię i nazwisko, adres zamieszkania lub pobytu, nr telefonu, adres e-mail,	14
11.	Kandydaci na ławników sądowych	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, Wizerunek, adres poczty elektronicznej, Nazwa i nr rejestru podmiotu zgłaszającego kandydata, motywy kandydowania	14
12.	Oświadczenia majątkowe	nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, zawód, informacja o posiadanych nieruchomościach wraz z adresami nieruchomości, informacja o nabytym mieniu od Skarbu Państwa, innej osoby prawnej, stan majątkowy	14
13.	Rejestr Gospodarki Odpadami	Nazwisko, imię, imiona, adres zamieszkania lub pobytu-kod pocztowy-miejscowość-ulica-nr domu lub mieszkania, PESEL, NIP, Regon, nr telefonu, e-mail, imiona rodziców, data urodzenia, dane współmałżonka, akt zgonu nr rachunku bankowego, nr identyfikacji	9
14.	Rejestr faktur i rachunków	Nazwisko, imię, imiona, adres zamieszkania lub pobytu-kod pocztowy-miejscowość-ulica-nr domu lub mieszkania, PESEL,data urodzenia, nr telefonu, e-mail, nr identyfikacji	3, 9
15.	Ewidencja wniosków i umów o zaopatrzenie w wodę i odprowadzanie ścieków	Nazwisko, imię, imiona, adres zamieszkania lub pobytu-kod pocztowy-miejscowość-ulica-nr domu lub mieszkania, PESEL, NIP, Regon, nr telefonu, e-mail, dane współmałżonka,	9
16.	Rejestr skazanych	Nazwisko, imię, imiona, adres	9

		zamieszkania lub pobytu-kod pocztowy-miejscowość-ulica-nr domu lub mieszkania, data i miejsce urodzenia, imiona rodziców	
17.	Windykacja należności cywilnoprawnych i publicznych	Nazwisko, imię, imiona, adres zamieszkania lub pobytu-kod pocztowy-miejscowość-ulica-nr domu lub mieszkania, PESEL, NIP, Regon, data urodzenia, nr telefonu, e-mail, imiona rodziców, dane współmałżonka, nr identyfikacji	3,4,5,6,7,9,10
18.	Podatki i opłaty lokalne	Nazwisko , imiona, imiona rodziców, adres zamieszkania i pobytu, data i miejsce urodzenia, PESEL, NIP, REGON, PKD, seria i nr dowodu osobistego, nr telefonu, e-mail, nr fax	3,5,9
19.	System Informacji Oświatowej	Imię, nazwisko, adres, pesel, data urodzenia, miejsce urodzenia, zawód, nr rachunku bankowego, imiona rodziców, nr telefonu, miejsce zatrudnienia,	16
20.	Zamówienia publiczne	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numer REGON, Numer Identyfikacji Podatkowej, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, numer konta bankowego, nr działki,	16
21.	Dofinansowanie prawodawcom kosztów kształcenia zawodowego młodocianych pracowników	Imię, nazwisko, data urodzenia, zawód, numer rachunku bankowego, nazwa firmy, pesel, oceny uczniów, informacje o otrzymanej pomocy de minimis, wynagrodzenie pracowników młodocianych	16
22.	Informacje o wyrobach zawierających azbest	Imię, nazwisko, adres, numer działki	16
23.	Wykaz partnerów Wieniawskiego Klastra Energii	Imię, nazwisko, adres, pesel, numer dowodu osobistego, numer telefonu, NIP, regon, nazwa firmy, numer KRS	16
24.	Decyzje o warunkach zabudowy oraz o ustaleniu celu publicznego	Imię, nazwisko, adres, numer działki	16,12
25.	Decyzje środowiskowe	Imię, nazwisko, adres, numer działki	16,12
26.	Przyłącza wodociągowe i kanalizacyjne	Imię, nazwisko, adres, numer działki	16,12

27.	Świadczenia Rodzinne	Nazwiska, imiona, data urodzenia, adres zamieszkania, numer telefonu, PESEL, numer i seria dokumentu tożsamości, obywatelstwo,rodzaj szkoły/ adres szkoły,dane pracodawcy, nr konta bankowego,dochody rodziny ubiegającej się o świadczenie,orzeczenia wydane w postępowaniu administracyjnym i sądowym, stan cywilny, stopień pokrewieństwa	4,6
28.	Fundusz i Zaliczka Alimentacyjna/ Dłużnicy alimentacyjni	Nazwiska, imiona,nazwiska, imiona rodziców, data urodzenia,miejsce urodzenia, adres zamieszkania , PESEL, NIP, nr konta bankowego dane pracodawcy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu,orzeczenia wydawane w postępowaniu administracyjnym lub sądowym, dane dotyczące skazań, stan zdrowia, stopień pokrewieństwa	4,6
29.	Zasiłek Dla Opiekuna	Nazwiska, imiona, data urodzenia,adres zamieszkania, numer telefonu, PESEL,nr i seria dokumentu tożsamości,nr konta bankowego, obywatelstwo, orzeczenia wydane w postępowaniu administracyjnym i sądowym, stan cywilny, stopień pokrewieństwa	4,6
30.	„ Za życiem"	Nazwiska, imiona,data urodzenia, adres zamieszkania, numer telefonu, PESEL, numer i seria dokumentu tożsamości,płeć, obywatelstwo,dane pracodawcy, nr konta bankowego,orzeczenia wydane w postępowaniu administracyjnym i sądowym, stan cywilny,	4,6
31.	Świadczenie wychowawcze	Nazwiska, imiona, adres zamieszkania, nr telefonu, nr PESEL,Nr i seria dokumentu tożsamości, obywatelstwo,rodzaj szkoły/ adres szkoły,dane pracodawcy, nr konta bankowego, dochody rodziny ubiegającej się o świadczenie,orzeczenia wydane w postępowaniu administracyjnym i sądowym, stan cywilny,płeć, stopień pokrewieństwa	4,6

32.	Karta Dużej Rodziny	Nazwiska, imiona, adres zamieszkania, nr telefonu, adres email,PESEL, nr i seria dokumentu tożsamości, obywatelstwo,orzeczenia wydane w postępowaniu administracyjnym i sądowym, dane odnośnie władzy rodzicielskiej, adres do korespondencji, stopień pokrewieństwa, dane szkoły	4,6
33.	USC Akta i Księgi Stanu Cywilnego, Orzekanie w sprawach zmian imion i nazwisk, Protokoły i zaświadczenia, Rejestr testamentów, PESEL, Projekty aktów i wzmianek, migracja aktów stanu cywilnego	Nazwisko i imię, imiona rodziców, nazwisko rodowe matki, data i miejsce urodzenia, adres zamieszkania lub adres pobytu, numer ewidencyjny PESEL, wykształcenie, seria i nr dowodu osobistego, data zgonu, miejsce zgonu, nazwisko noszone po zawarciu związku małżeńskiego, data i nr aktu urodzenia, małżeństwa, zgonu	20
34.	EL Rejestr mieszkańców, rejestr wyborców, rejestr cudzoziemców, spisy i statystyki, subskrypcje PESEL	Nazwiska i imiona, imiona rodziców, nazwisko rodowe rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, wykształcenie, miejsce byłego pobytu, przyczyna zmiany pobytu, obywatelstwo, płeć, seria i nr dowodu osobistego	20
35.	RDO - Rejestr dowodów osobistych	Fotografia, nazwisko i imię, nazwisko rodowe, imiona rodziców, nazwisko rodowe matki, data i miejsce urodzenia, adres do korespondencji, numer PESEL, płeć, obywatelstwo, powód ubiegania się o dowód osobisty	18, 20
36.	Kwalifikacja wojskowa	Nazwisko i imię, nazwisko rodowe, numer PESEL, data i miejsce urodzenia, miejsce pobytu stałego lub czasowego.	18
37.	Obrona Cywilna, Zarządzanie kryzysowe i sprawy obronne	Nazwisko i imiona, adres zamieszkania lub pobytu, miejsce pracy, numer telefonu, nazwa i adres jednostki organizacyjnej na rzecz której świadczenie ma być wykonane	18
38.	Archiwum zakładowe	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, numer NIP, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego, numer telefonu,	Podpiwniczenie

		inne dane -informacje zawarte w dokumentacji związanej z działalnością gminy	
39.	Zezwolenia na sprzedaż napojów alkoholowych	Imię, nazwisko, adres-kod pocztowy, miejscowość, ulica-nr domu lub mieszkania, NIP, nr telefonu	12
40.	Ewidencja działalności gospodarczej	Imię, nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres-kod pocztowy, miejscowość, ulica-nr domu lub mieszkania,, PESEL, NIP, REGON, seria i nr dowodu osobistego, nr telefonu, adres e-mail	12
41.	Zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	Imię, nazwisko, data urodzenia, miejsce urodzenia, adres-kod pocztowy, miejscowość, ulica-nr domu lub mieszkania,, PESEL, NIP, seria i nr dowodu osobistego, nr telefonu, nr rachunku bankowego, pow. użytków rolnych,	12
42.	Ewidencja przydomowych oczyszczalni ścieków i zbiorników bezodpływowych	Imię, nazwisko, adres-kod pocztowy, miejscowość, ulica-nr domu lub mieszkania, nr ewidencyjny działki,	12
43.	Ewidencja mienia komunalnego	Imię i nazwisko, adres zamieszkania, NIP, nr działki, obrębu, nr kw	10
44.	Gospodarka nieruchomościami	Imię i nazwisko, adres zamieszkania, PESEL, NIP, dane współmałżonka, nr działki	10
45.	Zarządzanie drogami	Imię i nazwisko, adres zamieszkania lub siedziby, NIP, REGON, nr działki,	10
46.	Rejestr nieruchomości stanowiących własność gminy	Imię i nazwisko, imiona rodziców, seria i nr dowodu osobistego, adres zamieszkania, dane współmałżonka PESEL, NIP, REGON, nr kw	10
47.	Szkody rolnicze	Imię i nazwisko, adres zamieszkania, nr identyfikacyjny, nr działek, nr telefonu	10
48.	Zbiór najemców lokali użytkowych i mieszkalnych	Imię i nazwisko, adres zamieszkania lub pobytu, PESEL, NIP, dane współmałżonka,lokalizacja nieruchomości, dane lokalu	10
49.	Zbiór nabywców nieruchomości	Imię i nazwisko, adres zamieszkania lub pobytu PESEL, dane współmałżonka, lokalizacja nieruchomości	10
50.	Rejestr wniosków i zgłoszeń na wycinkę	-nazwisko i imię, -adres zamieszkania lub pobytu,	10

	drzew	-numer ewidencyjny działki, - obręb ewidencyjny, -numer telefonu, -numer księgi wieczystej,	
51.	Wypis/wyrys z planu zagospodarowania przestrzennego oraz studium kierunków i zagospodarowania przestrzennego	-nazwisko i imię, -adres zamieszkania lub pobytu, -numer ewidencyjny działki, -obręb ewidencyjny, -numer telefonu	10
52.	Rozgraniczenie i podział nieruchomości	-nazwisko i imię, -adres zamieszkania lub pobytu, -numer ewidencyjny działki, -obręb ewidencyjny, -numer księgi wieczystej,	10
53.	Ochrona środowiska	-nazwisko i imię -adres zamieszkania lub pobytu, - numer ewidencyjny działki, -obręb ewidencyjny,	10
54.	Planowanie przestrzenne	-nazwisko i imię, -adres zamieszkania lub pobytu, -numer ewidencyjny działki, -obręb ewidencyjny,	10
55.	Rejestr dowodów księgowych	Nazwisko, imię, imiona, Nazwa kontrahenta, adres zamieszkania, adres siedziby, PESEL, NIP, REGON, kwota	3
56.	Rejestr VAT	Nazwisko, imię, imiona, Nazwa kontrahenta, adres zamieszkania, adres siedziby, PESEL, NIP, REGON, kwota	3
57.	Wspólnoty gruntowe	Nazwisko , imiona, imiona rodziców, adres zamieszkania i pobytu, data i miejsce urodzenia, PESEL, seria i nr dowodu osobistego, nr telefonu, e-mail, księgi wieczyste, powierzchnia nieruchomości, numer działki	5,10

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik Nr 2
do Zarządzenia Nr 12.2018
Wójta Gminy Wieniawa
z dnia 31 stycznia 2018 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania informacji prawnie chronionej, w tym danych osobowych w Urzędzie Gminy Wieniawa

Ilekroć w niniejszej instrukcji zostanie użyte poniższe sformułowanie, to należy przez to rozumieć:

- **ADO** - Administrator Danych Osobowych.
- **ABI** - Administrator Bezpieczeństwa Informacji.
- **ASI** - Administrator Systemów Informatycznych.
- **Przetwarzanie danych osobowych** - to: wpisywanie, kasowanie, kopiowanie, przenoszenie, modyfikowanie, dopisywanie, zapamiętywanie, filtrowanie według zadanych reguł.
- **System operacyjny (OS):** - zespół programów informatycznych zarządzających elektronicznym urządzeniem komputerowym.
- **Komputer (PC)** - urządzenie elektroniczne zarządzane systemem operacyjnym.
- **Dysk twardy, napęd dysku twardego** – rodzaj pamięci masowej, wykorzystujący nośnik magnetyczny do przechowywania danych.
- **Drzewo katalogów** - graficzna interpretacja organizacji dysku komputera.
- **Program dziedzinowy** - to: zbiór instrukcji i poleceń zapisany w języku programowania elektronicznych urządzeń komputerowych, wykonujących procesy przetwarzania informacji z zadanych dziedzin.
- **Identyfikator użytkownika PC** - jest to unikalny zestaw znaków, opisujący tylko tego jednego użytkownika niezbędny do pracy w systemie informatycznym (IT),
- **użytkownik uprzywilejowany** – administrator systemu PC

1. Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności:

1.1. Prawo do pracy na stanowisku komputerowym nadaje ADO stosownym upoważnieniem, ASI nadaje login i hasło do systemu operacyjnego na stanowisku komputerowym.

1.2. Pełne uprawnienia do przetwarzania danych w systemie informatycznych programów dziedzinowych nadaje ADO na wniosek kierownika komórki organizacyjnej, za pośrednictwem ABI.

1.3. Rejestr osób uprawnionych do przetwarzania danych oraz zakres ich uprawnień jest prowadzony w wersji elektronicznej przez ABI.

1.4. Po nadaniu uprawnień do przetwarzania danych, ABI przyznaje użytkownikowi danych unikalne

identyfikator i hasło dostępu do systemu programów dziedzinowych.

2. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem:

2.1. Uzyskanie dostępu do systemu dziedzinowego przetwarzania danych osobowych następuje wyłącznie poprzez podanie prawidłowego identyfikatora i hasła, przyznanych użytkownikowi podczas procesu udzielania upoważnień do przetwarzania danych osobowych i przyznawania uprawnień do systemu informatycznego. Hasło nadane przez ASI musi składać się z co najmniej 8 znaków, zawierać małe i duże litery oraz cyfry a także może zawierać inne wszelkie znaki graficzne bezpośrednio dostępne z klawiatury komputera.

2.2. Użyty identyfikator nie może być powtórnie przyznany innemu użytkownikowi.

2.3. Zabronione jest stosowanie jako haseł: nazw prostych/własnych, (imion osób, imion zwierząt, nazw drużyn piłkarskich, nazw zespołów muzycznych, nazw marek samochodów, nazw obiektów geograficznych) dat urodzin, nazw miejscowości, nazwiska lub imienia użytkownika lub jego bliskich, lub innych bliskoznacznych zwrotów i wyrazów wcześniej przytoczonych.

2.4. Należy stosować trudne do odgadnięcia (nie słownikowe) ciągi znaków spełniające warunki jak w pkt.2.1.

2.5. Hasła nie mogą być:

a) zapisane jawnie i umieszczone w miejscu widocznym dla każdej z osób przebywającej w pobliżu operatora komputera,

b) przekazywane ani przesyłane za pomocą telefonu, faksu ani poczty e- mail w formie jawnej.

2.6. Szczególne ustawienia systemu operacyjnego:

a) Zabronione jest dla użytkowników anonimowe logowanie do systemu.

b) System informatyczny nie może podpowiadać ani wyświetlać żadnych informacji opisujących, konfigurację sieci lub innych informacji dotyczących bezpieczeństwa danych.

c) Uwierzytelnienie następuje wyłącznie po prawidłowym wpisaniu w polu logowania hasła i powiązanego z nim identyfikatora użytkownika danych.

3. Regulamin posługiwania się hasłem i loginem:

3.1. Użytkownik danych, któremu przypisano identyfikator i hasło zobowiązany jest do przestrzegania następujących zasad:

a) Powierzony identyfikator i hasło nie może znajdować się w miejscu widocznym dla osób nieupoważnionych (np. zawieszone na monitorze).

b) Niedopuszczalne jest uwierzytelnianie się („logowanie się") na identyfikator i hasło innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.

c) Zabrania się udostępniania przydzielonego osobistego identyfikatora i hasła, stanowiska pracy

i istniejących na nim danych innym użytkownikom a także osobom nieupoważnionym.

4. Procedura zarządzania ryzykiem:

a) W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się" w systemie) lub działania systemu, użytkownik niezwłocznie powiadamia o nich ABI, który ma obowiązek zapoznać się z przekazanymi uwagami oraz podjąć odpowiednie działania opisane w punkcie 7.

b) Użytkownicy systemu zobowiązani są do ochrony wprowadzanych danych przez zabezpieczenie ekranu monitora przed wzrokiem nieupoważnionych osób.

c) Niedopuszczalna jest sytuacja, gdy ekran monitora osoby wprowadzającej dane osobowe skierowany jest w stronę osób nieupoważnionych.

d) Po zakończeniu operacji, użytkownik obowiązany jest wylogować się z systemu.

e) W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych, każdy z użytkowników obowiązany jest niezwłocznie powiadomić o tym ABI.

f) Hasło dostępu do systemu należy zmieniać w cyklu 30-to dniowym.

g) Zabrania się ponownego stosowania haseł stosowanych w przeszłości.

h) Nie wolno wykorzystywać sieci komputerowej w celach innych niż wyznaczone przez ABI.

i) Na zestawach komputerowych użytkownikowi nie wolno instalować i używać samowolnie zainstalowanych programów informatycznych.

j) Zabrania się trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie.

k) Zabrania się rozpowszechniania programów komputerowych lub ich kopii dla osób postronnych.

l) Zabrania się tłumaczenia, dekompilacji, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym.

m) Zabrania się używania oprogramowania, które posiada sfałszowane znaki firmowe lub nie posiada w ogóle znaków firmowych, etykiet, oryginalnych nośników, dokumentacji łącznie z elektroniczną.

n) Zabrania się udostępniania osobom postronnym programów komputerowych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu.

o) Zabrania się używania oprogramowania w większym zakresie niż pozwala na to umowa licencyjna (np. kopiowania programu, zmiany nazwy programu itp.);

p) Zabrania się kopiowania i wgrywania programów przynoszonych spoza urzędu na nośnikach magnetycznych lub CD bez zgody ABI.

q) Zabrania się udostępniania poza teren urzędu kopii plików i programów działających w sieci urzędu.

r) Zabrania się kopiowania na nośniki informatyczne drzewa katalogowego, dysków, zestawów

komputerów urzędu.

s) Zabrania się wgrywania, instalowania i użytkowania gier komputerowych oraz innych programów nie związanych z działalnością urzędu.

t) Zabrania się tworzenia nazw plików i katalogów (folderów) dłuższych niż 32 znaki ze spacjami włącznie;

u) Zabrania się samodzielnych napraw programów, sprzętu komputerowego oraz drukarek.

5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemach informatycznych przeznaczone dla użytkowników systemu:

5.1. Użytkownik rozpoczyna pracę w systemie od następujących czynności:

a) włączenia komputera,

b) Użytkownik loguje się do stacji roboczej za pomocą identyfikatora i hasła niezbędnego do autoryzacji dostępu do stacji roboczej.

c) Uwierzytelnienie się („zalogowania się") w systemie operacyjnym stanowiska komputerowego nastąpi wyłącznie po prawidłowym podaniu identyfikatora i hasła rozpoznanego przez system autentykacji systemu stanowiska komputerowego.

d) W systemie operacyjnym stacji roboczej uruchamia zgodnie z nadanymi uprawnieniami odpowiedni program dziedzinowy przeznaczony do przetwarzania informacji w tym danych osobowych.

e) Program dziedzinowy wyświetla formularz logowania lub znak zachęty.

f) Użytkownik podaje dane autoryzacyjne, identyfikator oraz hasło.

g) Dane są porównywane z bazą identyfikatorów i powiązanych z nimi haseł.

h) Jeśli identyfikator i hasło są tożsame – użytkownik jest dopuszczony do pracy

i) Użytkownik ma obowiązek zamykania systemu operacyjnego (wylogowanie) oraz programu użytkowego po zakończeniu pracy.

j) Zakończenie pracy użytkownika w systemie następuje po zamknięciu sesji w aplikacji dziedzinowej i następnie po zamknięciu sesji systemu operacyjnego na stacji roboczej użytkownika. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności nośniki danych (np. dyskietki, płyty CD, DVD, pendrive-y), dokumenty i wydruki zawierające dane osobowe przed dostępem osób nieupoważnionych.

k) Po zakończeniu pracy, na stanowisku obowiązuje zasada "czystego biurka".

l) W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się" lub zaktywizować wygaszasz ekranu z opcją ponownego „logowania" się do systemu.

m) Stanowisko komputerowe z uruchomionym systemem operacyjnym oraz programem użytkowym nie może pozostawać bez kontroli pracującego na nim użytkownika.

6. Procedury tworzenia kopii zapasowych zbiorów danych, kopii programów użytkowych i narzędzi programowych, archiwizacja:

6.1. Zintegrowany system modułów aplikacji użytkowych wykonuje automatycznie, codziennie podstawowe archiwalne kopie zbiorów danych. ASI kontroluje wykonanie procedury archiwizacji baz danych oraz uzupełnia archiwum baz danych nie objętych automatyczna archiwizacją.

6.2. W cyklu 7 dniowym ASI wykonuje zapis najnowszej wersji wszystkich kopii zapasowych na zewnętrznym, pozaserwerowym systemie dyskowym.

6.3. Pełne kopie danych z wszystkich aplikacji użytkowych przetwarzające informacje prawnie chronione, w tym dane osobowe, ASI poddaje kompresji i pliki wynikowe zgrywa na dysk przenośny.

6.4. Informacje prawnie chronione, w tym dane osobowe, przetwarzane w lokalizacji ul. Kochanowskiego 88, 26-432 Wieniawa są kopiowane i archiwizowane w trybie miesięcznym, indywidualnie przez operatorów stanowisk komputerowych poprzez zgrywanie na CD/DVD z plikami tych informacji. Skopiowane informacje na CD/DVD są przekazywane ASI.

6.5. Informacje prawnie chronione w lokalizacji, w tym dane osobowe z zakresu art. 27 ustawy o ochronie danych osobowych, przetwarzane w lokalizacji ul. Kochanowskiego 88, 26-432 Wieniawa elektronicznie składowane są na zewnętrzny dysk HDD. Po zakończeniu pracy dysk jest odłączany od systemu IT i przechowywany w zamykanej szafie w miejscu wytworzenia.

6.6. Informacje przetwarzane lub wytwarzane w aplikacjach biurowych, które nie posiadają stabilnej zdolności zapisu sieciowego (MS WORD/EXCEL), są kopiowane przez operatorów stanowisk komputerowych w trybie miesięcznym. Operatorzy stanowisk mają obowiązek kopiować dane zewnętrzny dysk HDD

6.7. Zawartość strony internetowej gminy Wieniawa jest kopiowana na serwerze Starostwa Powiatowego w Przysusze.

6.8. Nagrywanie oraz odsłuch rozmów telefonicznych zostanie uregulowane odrębnym zarządzeniem wójta, po wdrożeniu tego typu funkcjonalności.

6.9. Monitoring wizyjny będzie prowadzony nie później niż 25 maja 2018r., przy pomocy instalacji kamer telewizji przemysłowej typ CCTV oparty jest na dedykowanych rejestratorach sprzętowych. Informacja zapisana na nośnikach, zainstalowanych w tych rejestratorach, indeksowana jest datą i czasem, a sposób kompresji tej informacji nie daje możliwości manipulacji materiałem zapisu bez pozostawienia śladów. Po zapełnieniu obszaru zapisu dysku HDD rejestratora, nowa treść nadpisuje obszar najstarszego zapisu.

6.10. Kopie zapasowe przechowywane są w ściśle określonym, chronionym miejscu, do którego mają dostęp tylko ADO, ABI i ASI. Miejsce to powinno być różne od miejsca przechowywania zbiorów danych, z których sporządzono kopie zapasowe.

6.11. Wydruki zawierające dane osobowe są przechowywane w miejscu uniemożliwiającym ich odczytanie przez osoby nieuprawnione.

6.12. Wydruki tymczasowe, pomocnicze, nieprzydatne lub które straciły ważność a zawierają informacje prawnie chronione, są zniszczone w niszczarce dokumentów z odpowiednią klasą bezpieczeństwa określoną w odrębnych przepisach resortowych danego dokumentu w stopniu uniemożliwiającym ich odczytanie.

6.13. Tworzenie kopii zapasowych, innych niż zbiory danych osobowych przetwarzanych w systemie elektronicznym wykonywane jest automatycznie przez system operacyjny.

7. Procedury niszczenia nośników zawierających informacje z bazy danych osobowych po zakończeniu okresu ich użytkowania:

7.1. Dyski twarde, których wskutek uszkodzenia nie da się uruchomić w serwerze lub stacji roboczej pod nadzorem ABI niszczy się komisyjnie w jeden z poniżej podanych sposobów poprzez:

a) Fizyczny demontaż głównych podzespołów dysku twardego - płyta sterująca (elektronika), talerze nośnika danych (tarcze dysku twardego).

b) Fizyczne nieodwracalne zniszczenie elektroniki - np. zmiażdżenie młotkiem układów scalonych na płytce sterującej dyskiem;

c) Wykonanie otworów za pomocą wiertarki we wszystkich tarczach dysku twardego w sposób asymetryczny,

d) Przekazanie w całości do zniszczenia dysków twardych wyspecjalizowanej firmie zewnętrznej posiadającej wymagane prawem certyfikaty bezpieczeństwa.

e) Dyski twarde, które po zakończeniu eksploatacji da się uruchomić po decyzji ABI, niszczy się w sposób opisany powyżej lub stosuje się program do nadpisywania danych na całym obszarze przestrzeni dyskowej, który skutecznie uniemożliwi odczyt poprzednich danych zawartych na dysku.

f) Magnetyczne oraz optyczne (CD/CD-ROM) nośniki kopii zapasowych, po zaprzestaniu ich użytkowania, są niszczone w mechanicznych urządzeniach niszczących sposób uniemożliwiający ich użycie.

8. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest nieuprawniony dostęp do systemu informatycznego:

8.1. Sprawdzanie obecności wirusów komputerowych oraz programów, których celem jest nieuprawniony dostęp do systemu, dokonywane jest poprzez licencjonowany zainstalowany program antywirusowy, który skanuje automatycznie bez udziału użytkownika komputer. Program taki jest zainstalowany na wszystkich serwerach i stacjach roboczych.

8.2. Podczas uruchomienia systemu, program sprawdza wersję posiadanego programu antywirusowego i w razie konieczności dokonuje automatycznej aktualizacji do najnowszej wersji.

8.3. Po każdej naprawie i konserwacji komputera dokonuje się sprawdzenia pod kątem występowania wirusów i ponownie zainstaluje aktualne oprogramowanie antywirusowe.

8.4. Elektroniczne nośniki informacji pochodzenia zewnętrznego obowiązkowo podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.

9. Sposób realizacji wymogu rejestracji informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia:

9.1. Użytkownik systemu dziedzinowego, zapisuje w rejestrze prowadzonym w formie papierowej informacje o odbiorcach danych osobowych w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

10. Procedura wykonania przez ASI przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

10.1. Przeglądy i konserwacje systemu i zbiorów wykonywane są na bieżąco, lecz nie rzadziej niż raz w miesiącu. Sprawdzona zostaje spójność danych, indeksów oraz stan nośników np. dysków twardych.

10.2. Okresowo (nie rzadziej niż raz na miesiąc) sprawdzona zostaje możliwość odtworzenia danych z kopii zapasowej.

10.3. Naprawy serwisowe sprzętu objętego umowami serwisowymi wykonywane są (bez nośników informacji "dysków twardych, pamięci masowej - HDD") zgodnie z zasadami ustalonymi w umowie serwisowej.

10.4. Naprawa sprzętu z danymi chronionymi, która odbywa się w miejscu jego użytkowania, wykonywana jest pod nadzorem ASI lub za zgodą ABI, w obecności osób użytkujących sprzęt.

10.5. Sprzęt komputerowy przed oddaniem do serwisu poza miejsce jego użytkowania, jest odpowiednio przygotowany. Informacje prawnie chronione są zarchiwizowane na nośniki zewnętrzne, a z dysków twardych skutecznie usuwane zbiory danych i programy użytkowe.

10.6. Niedopuszczalne jest przekazanie do naprawy poza siedzibę urzędu uszkodzonego elementu, na którym są przechowywane dane chronione.

10.7. Zmiana konfiguracji sprzętu komputerowego lub zmiana jego lokalizacji może być dokonana tylko przez ASI za zgodą ABI.

WÓJT

mgr inż. Krzysztof Sobczak