Zarządzenie Nr 9/2010

Wójta Gminy Olszówka

z dnia 01.10.2010 r.

w sprawie ustalenia „Polityki bezpieczeństwa informacji" i „Instrukcji określającej sposób zarządzania systemem informatycznym Urzędu Gminy w Olszówce"

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.) oraz §3 ust.3, §4 i 5 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 (Dz. U. Nr 100, poz.1024), zarządza się, co następuje:

§1. Ustalam „Politykę bezpieczeństwa informacji", w brzmieniu załącznika Nr 1 do niniejszego zarządzenia oraz „Instrukcję określającą sposób zarządzania systemem informatycznym Urzędu Gminy w Olszówce", która stanowi załącznik Nr 2 do zarządzenia.

§2. Zobowiązuję pracowników Urzędu Gminy w Olszówce do stosowania zasad określonych w „Polityce bezpieczeństwa informacji" oraz „Instrukcji określającej sposób zarządzania systemem informatycznym Urzędu Gminy w Olszówce".

§3. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1
do Zarządzenia Nr 9/2010
Wójta Gminy Olszówka
z dnia 01.10.2010 r.

Polityka Bezpieczeństwa Informacji

Urzędu Gminy w Olszówce

Spis treści

1. Wstęp

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Urząd Gminy w Olszówce przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka określa obowiązki Administratora Danych Osobowych w zakresie zabezpieczenia danych osobowych o których mowa w § 36 Ustawy o Ochronie Danych Osobowych.

Polityka określa reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych w postaci papierowej oraz zawartych w systemach informatycznych w Urzędzie Gminy w Olszówce.

Integralną częścią niniejszej polityki jest Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją zarządzania systemem informatycznym". Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Polityka została opracowana zgodnie z wymogami określonymi w § 4 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 (Dz. U. Nr 100, poz. 1024).

Polityka obowiązuje wszystkich pracowników Urzędu Gminy w Olszówce oraz dostawców, podmiotów współpracujących na zasadzie umów, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Za przestrzeganie zasad ochrony i bezpieczeństwa danych w Urzędzie Gminy w Olszówce odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2002r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004r. Nr 25, poz. 219 i Nr 33, poz. 285)
2. Rozporządzeniem 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. Nr 100, poz. 1024)

2. Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka – rozumie się przez to Politykę Bezpieczeństwa Informacji Urzędu Gminy Olszówka.
2. Administrator Danych Osobowych (ADO) – Wójt Gminy Olszówka, decydujący o celach i środkach przetwarzania danych osobowych;
3. Administrator Bezpieczeństwa Informacji (ABI) – pracownik Urzędu Gminy w Olszówce, wyznaczony przez Wójta Gminy Olszówka, odpowiedzialny za organizację ochrony danych osobowych;
4. Kierownik – osoba pełniąca funkcje kierownicze w Urzędzie Gminy w Olszówce;
5. Ustawa – rozumie się przez to ustawę z dnia 29 sierpnia.1997 r. o ochronie danych osobowych (Dz. U. z 1997 r. Nr 133, poz.883);
3. Rozporządzenie – rozumie się przez to rozporządzenie 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. Nr 100, poz. 1024);
6. Dane osobowe (dane) – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów np. zbiór petentów Urzędu Gminy w Olszówce, zbiór osób przekazujących swoje oferty pracy, zbiór pracowników Urzędu Gminy w Olszówce;
8. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
9. Zgoda osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
10. Baza danych osobowych – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisane dane osobowe;
11. Przetwarzanie danych – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
12. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
13. Administrator Systemu Informatycznego (ASI) – osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
14. Użytkownik – pracownik Urzędu Gminy w Olszówce posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
15. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,
16. Nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde;

3. Regulamin Administratora Bezpieczeństwa Informacji

Do najważniejszych obowiązków Administratora Bezpieczeństwa Informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki,
3. wydawanie i anulowanie upoważnień do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład dla osób przetwarzających dane osobowe,
4. prowadzenie „Rejestru osób zatrudnionych przy przetwarzaniu danych osobowych",
5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6. nadzór nad bezpieczeństwem danych osobowych,
7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych w Urzędzie Gminy w Olszówce,

Administrator Bezpieczeństwa Informacji ma prawo:

1. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
2. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
3. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
4. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

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

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, opisane jest w Załączniku A „Wykaz zbiorów danych osobowych".

5. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany jest w Załączniku A „Wykaz zbiorów danych osobowych".

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

1. W ramach programu Radix Kadry przetwarzane są dane osobowe pracowników Urzędu Gminy w Olszówce obejmujące:

   - imię (imiona) i nazwisko;
   - adres zameldowania, zamieszkania i do korespondencji;
   - datę i miejsce urodzenia;
   - płeć;
   - wykształcenie;
   - numery PESEL i NIP;
   - imiona rodziców;
   - zwolnienia lekarskie;
   - Urząd Skarbowy;
   - wysokość wynagrodzenia;
   - stan cywilny;
   - podleganie służbie wojskowej;
   - posiadanie gospodarstwa rolnego;
   - warunki zatrudnienia;
   - historia przebiegu pracy zawodowej.

2. W ramach systemu „Płatnik" przetwarzane są w formie elektronicznej i papierowej dane osobowe pracowników oraz osób współpracujących z Urzędem Gminy w Olszówce na podstawie umów zleceń i umów o dzieło obejmujące:

   - imię (imiona) i nazwisko;
   - nazwisko rodowe
   - adres zameldowania, zamieszkania i do korespondencji;
   - datę urodzenia;
   - numery PESEL i NIP;

- numer dowodu osobistego;
- obywatelstwo;
- stopień niepełnosprawności.

3. W ramach prowadzonych rekrutacji do pracy w Urzędzie Gminy w Olszówce przetwarzane są w formie papierowej następujące dane osobowe uczestników tych procesów:

   - imię (imiona) i nazwisko;
   - imiona rodziców;
   - data urodzenia;
   - obywatelstwo;
   - miejsce zamieszkania (adres do korespondencji);
   - wykształcenie (nazwa szkoły i rok jej ukończenia, zawód, specjalność, stopień naukowy, tytuł zawodowy, tytuł naukowy);
   - wykształcenie uzupełniające (kursy, studia podyplomowe, data ukończenia nauki lub data rozpoczęcia nauki w przypadku jej trwania);
   - przebieg dotychczasowego zatrudnienia (okresy zatrudnienia u kolejnych pracodawców oraz zajmowane stanowiska pracy);
   - dodatkowe uprawnienia, umiejętności, zainteresowania (np.: stopień znajomości języków obcych, prawo jazdy, obsługa komputera);
   - oświadczenie o pozostawaniu/nie pozostawaniu w rejestrze bezrobotnych i poszukujących pracy;
   - oświadczenie o zgodności danych z dowodem osobistym (seria i numer) wydanym przez (nazwa uprawnionego organu) lub innym dowodem tożsamości.

Dane są przechowywane przez 24 miesiące.

4. W momencie zatrudnienia w oparciu o umowę o pracę kandydata do pracy w formie papierowej i elektronicznej przetwarzane są jego następujące dane osobowe:

   - imię (imiona) i nazwisko;
   - nazwisko rodowe;
   - adres zameldowania, zamieszkania i do korespondencji;
   - telefon kontaktowy;
   - datę urodzenia;
   - miejsce urodzenia;
   - obywatelstwo;
   - numery PESEL i NIP;
   - przynależności do oddziału Narodowego Funduszu Zdrowia;
   - dotyczące służby wojskowej (stosunek do powszechnego obowiązku obrony, stopień wojskowy, numer specjalności wojskowej, przynależność ewidencyjna do WKU, numer książeczki wojskowej, przydział mobilizacyjny do sił zbrojnych RP);
   - wskazania osób wraz z danymi kontaktowymi do powiadomienia w razie wypadku;

5. Na potrzeby wydania legitymacji ubezpieczeniowej osobie zatrudnionej oraz dla członków rodziny pracownika przetwarzane są następujące dane osobowe w formie papierowej:

   - imię i nazwisko pracownika;
   - adres zamieszkania pracownika;
   - imiona rodziców pracownika;
   - data i miejsce urodzenia pracownika ;
   - miejsce zatrudnienia pracownika;
   - seria i numer dowodu osobistego pracownika;
   - numer legitymacji ubezpieczeniowej pracownika;
   - imię i nazwisko członka rodziny zgłaszanego do ubezpieczenia zdrowotnego;
   - data urodzenia członka rodziny zgłaszanego do ubezpieczenia zdrowotnego;
   - stopień pokrewieństwa z osobą zgłaszaną do ubezpieczenia zdrowotnego;
   - adres zamieszkania członka rodziny zgłaszanego do ubezpieczenia zdrowotnego;
   - stan cywilny członka rodziny zgłaszanego do ubezpieczenia zdrowotnego;
   - seria i numer dowodu osobistego;
   - numer legitymacji ubezpieczeniowej dla członków rodziny

6. Na potrzeby zgłoszenia osoby zatrudnionej do ubezpieczenia zbiorowego przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

   - imię i nazwisko;
   - adres zamieszkania;
   - data i miejsce urodzenia;
   - numer PESEL;
   - telefon kontaktowy;
   - imię i nazwisko osoby uposażonej;
   - adres do korespondencji osoby uposażonej.

7. W momencie przyjęcia przez pracodawcę młodocianego pracownika na dokształcenie w formie papierowej i elektronicznej przetwarzane są następujące dane osobowe:

   - imię (imiona) i nazwisko wnioskodawcy;
   - adres zamieszkania;
   - numer PESEL;
   - numer telefonu;
   - numer rachunku bankowego pracodawcy;
   - nazwa i adres zakładu pracy;
   - imie i nazwisko młodocianego pracownika;
   - adres zamieszkania młodocianego pracownika;
   - miejsce i adres realizacji przez młodocianego obowiązkowego dokształcania teoretycznego;
   - data zawarcia umowy o pracę oraz okres kształcenia wynikający z umowy o pracę;
   - data i miejsce zdania egzaminu zawodowego.

8. W ramach systemu Radix ELUD oraz w formie papierowej przetwarzane są dane osobowe mieszkańców gminy Olszówka, którzy zgłaszają wniosek o wydanie dowodu osobistego, obejmujące:

- imię (imiona) i nazwisko;
- nazwisko rodowe;
- imiona rodziców;
- nazwisko rodowe matki;
- data urodzenia;
- miejsce urodzenia;
- stan cywilny;
- numer PESEL;
- kolor oczu;
- wzrost;
- płeć;
- adres zamieszkania;
- seria i numer posiadanego dokumentu tożsamości;
- nazwa i siedziba podmiotu, który wydał dokument;
- powód wymiany dowodu;
- data utracenia dowodu;
- przyczyna utraty dowodu;
- fotografia;
- uprzedzenie o odpowiedzialności karnej z art. 272 Kodeksu Karnego za fałszywe zeznania, prawdziwość spisanych danych.

9. W ramach systemu Radix ELUD oraz w formie papierowej przetwarzane są dane osobowe mieszkańców gminy Olszówka w celach meldunkowych obejmujące:

- imię (imiona) i nazwisko;
- data i miejsce urodzenia;
- imiona rodziców;
- nazwiska rodowe rodziców;
- adres zamieszkania;
- adresy wcześniejszego zamieszkania;
- numer PESEL;
- numer i seria dowodu osobistego;
- uprawnienia do wyborów;
- numer książeczki wojskowej;
- stan cywilny;
- imię (imiona) i nazwisko współmałżonka;
- nazwisko rodowe współmałżonka;
- wykształcenie;
- poprzednie nazwiska;
- obywatelstwo.

10. Na potrzeby stworzenia listy osób podlegających stawieniu się do kwalifikacji wojskowej w formie papierowej przetwarzane są następujące dane osobowe:

- imię (imiona) i nazwisko kwalifikowanego;
- data i miejsce urodzenia;
- imię ojca;
- adres zamieszkania;
- stan cywilny;

- numer książeczki wojskowej;
- kategoria zdolności do czynnej służby wojskowej.

11. Na potrzeby wykonywania czynności z zakresu rejestracji stanu cywilnego przetwarzane są następujące dane osobowe w formie papierowej:

- termin zawarcia małżeństwa;
- imię (imiona) i nazwisko;
- nazwisko rodowe;
- stan cywilny;
- data i miejsce urodzenia;
- imię (imiona) i nazwisko ojca;
- nazwisko rodowe ojca;
- imię (imiona) i nazwisko matki;
- nazwisko rodowe matki;
- numer aktu urodzenia;
- numer aktu wcześniejszego małżeństwa;
- dane sądu udzielającego rozwód;
- sygnatura wyroku;
- dane z aktu zgonu małżonka;
- numer dowodu osobistego;
- numer PESEL;
- miejsce zamieszkania;
- numer telefonu;
- imię (imiona), nazwisko i nazwisko rodowe osoby, z którą planowany jest ślub
- oświadczenie o nie pozostawaniu w innym związku małżeńskim;
- oświadczenie o braku pokrewieństwa lub powinowactwa w linii prostej, braku stosunku przysposobienia, braku pokrewieństwa typu rodzeństwo rodzone lub przyrodnie;
- oświadczenie dotyczące zmiany nazwiska po ślubie;
- oświadczenie o nadaniu nazwiska dzieciom po ich urodzeniu.

12. W formie papierowej przetwarzane są dane osobowe czytelników biblioteki w Olszówce obejmujące:

- imię (imiona) i nazwisko;
- numer czytelnika;
- znak statystyczny;
- data urodzenia;
- numer PESEL;
- zawód/miejsce pracy;
- szkoła, klasa;
- adres zamieszkania;
- adres zameldowania;
- numer telefonu;
- imię ojca;
- upoważnienie do korzystania z konta osobie trzeciej – imię i nazwisko, adres zameldowania, telefon.

13. W momencie zgłoszenia się do Urzędu Gminy w Olszówce petenta, który otwiera/posiada działalność gospodarczą przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej w programie Sputnik EDG (ewidencja działalności gospodarczej):

- płeć;
- rodzaj, seria i numer dokumentu tożsamości;
- numer PESEL;
- numer NIP;
- REGON;
- imię (imiona) i nazwisko;
- nazwisko rodowe;
- imiona rodziców;
- data i miejsce urodzenia;
- obywatelstwo;
- adres miejsca zamieszkania;
- adres miejsca zameldowania;
- nazwa działalności gospodarczej;
- data rozpoczęcia działalności gospodarczej;
- rodzaj działalności gospodarczej;
- adres głównego miejsca wykonywania działalności;
- adres do korespondencji;
- numer telefonu;
- numer faksu;
- adres poczty elektronicznej;
- dane dla potrzeb KRUS;

14. Na potrzeby wydania pozwolenia na alkohol przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej w systemie DON (dziennik obrotów nieprzypisanych):
- imię (imiona) i nazwisko;
- adres zamieszkania;
- adres punktu sprzedaży

15. Na potrzeby realizowania profilaktyki alkoholowej i przeciwdziałania narkomanii przetwarzane są następujące dane osobowe w formie papierowej:
- imię (imiona) i nazwisko;
- imiona rodziców;
- adres zamieszkania;
- data urodzenia;
- numer PESEL.

16. W momencie złożenia oświadczenia majątkowego pracownika lub radnego Urzędu Gminy w Olszówce przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- imię (imiona) i nazwisko;
- nazwisko rodowe;
- data i miejsce urodzenia;
- miejsce zatrudnienia;

- stanowisko lub funkcja;
- posiadane zasoby pieniężne;
- posiadane nieruchomości;
- posiadane udziały w spółkach handlowych;
- posiadane akcje w spółkach handlowych;
- nabyte mienia;
- prowadzone działalności gospodarcze;
- funkcje pełnione w spółkach handlowych, spółdzielniach, fundacjach;
- inne dochody;
- składniki mienia ruchomego;
- zobowiązania pieniężne;
- adres zamieszkania;
- miejsce położenia nieruchomości.

17. W ramach programu księgowego FKJ Radix oraz w formie papierowej przetwarzane są dane osobowe:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- numer NIP;

18. W ramach programu Radix Pogrun oraz w formie papierowej na potrzeby naliczania podatku rolnego przetwarzane są następujące dane osobowe:
- imię (imiona) i nazwisko;
- adres zamieszkania;
- data i miejsce urodzenia;
- imiona rodziców;
- numer PESEL;
- numer NIP;
- powierzchnia gruntów.

19. W ramach programu Radix Pogrun oraz w formie papierowej na potrzeby naliczania podatku leśnego przetwarzane są następujące dane osobowe:
- imię (imiona) i nazwisko;
- adres zamieszkania;
- data i miejsce urodzenia;
- imiona rodziców;
- numer PESEL;
- numer NIP;
- powierzchnia lasów.

20. W ramach programu Radix Pogrun oraz w formie papierowej na potrzeby naliczania podatku od nieruchomości przetwarzane są następujące dane osobowe:
- imię (imiona) i nazwisko;
- adres zamieszkania;
- data i miejsce urodzenia;
- imiona rodziców;
- numer PESEL;
- numer NIP;
- powierzchnia budynków.

21. W ramach programu Radix WIP oraz w formie papierowej na potrzeby naliczania podatku transportowego przetwarzane są następujące dane osobowe:
   - imię (imiona) i nazwisko;
   - adres zamieszkania;
   - data i miejsce urodzenia;
   - imiona rodziców;
   - numer PESEL;
   - numer NIP;
   - numer rejestracyjny pojazdu.

22. Na potrzeby prowadzenia rejestru płaconych czynszów za lokale mieszkalne i użytkowe w formie papierowej przetwarzane są następujące dane osobowe:

   - imię (imiona) i nazwisko;
   - adres zamieszkania;
   - numer i seria dowodu osobistego;

23. Na potrzeby wyliczenia zwrotu podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej w formie papierowej przetwarzane są następujące dane osobowe:
   - imię (imiona) i nazwisko;
   - adres zamieszkania;
   - numer i seria dowodu osobistego;
   - numer PESEL;
   - numer NIP;
   - powierzchnia gruntów;
   - numer konta bankowego.

24. Na potrzeby wystawienia zaświadczenia o niezaleganiu w podatkach w formie papierowej przetwarzane są następujące dane osobowe:
   - imię (imiona) i nazwisko;
   - adres zamieszkania;
   - numer NIP;
   - data urodzenia.

25. Na potrzeby wystawienia zaświadczenia o figurowaniu w rejestrze podatników w formie papierowej przetwarzane są następujące dane osobowe:
   - imię (imiona) i nazwisko;
   - adres zamieszkania;
   - powierzchnia gospodarstwa.

26. Na potrzeby prowadzenia rejestru wniosków o przyznanie stypendium przetwarzane są następujące dane osobowe w formie papierowej:

   - imię (imiona) i nazwisko wnioskodawcy;
   - adres zamieszkania wnioskodawcy;
   - telefon kontaktowy wnioskodawcy;
   - imię i nazwisko ucznia;
   - data miejsce urodzenia ucznia;

- adres zamieszkania ucznia;
- klasa i szkoła, do której uczęszcza dziecko;
- numer PESEL wszystkich członków rodziny;
- stopień pokrewieństwa;
- miejsce zatrudnienia/nauki;
- wysokość osiąganych dochodów.

27. Na potrzeby prowadzenia rejestru wydanych decyzji odnośnie przyznania stypendium przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej w programie Pomoc Materialna dla Uczniów (Sputnik):
- imię (imiona) i nazwisko ucznia;
- adres zamieszkania;
- imiona i nazwiska wnioskodawcy;
- adres zamieszkania wnioskodawcy;
- wysokość osiąganych dochodów;
- wysokość świadczenia.

28. Na potrzeby prowadzenia rejestru uczniów, którzy otrzymują wyprawki szkolne przetwarzane są następujące dane osobowe w formie papierowej:

- imię (imiona) i nazwisko rodziców;
- adres zamieszkania;
- imię (imiona) i nazwisko dziecka;
- klasa i szkoła uczęszczania;
- numer konta bankowego.

29. Na potrzeby podpisania umowy z rodzicami na zwrot dojazdu dzieci do szkół podstawowych i gimnazjalnych przetwarzane są następujące dane osobowe w formie papierowej:
- imię (imiona) i nazwisko rodzica;
- adres zamieszkania;
- imię i nazwisko dziecka.

30. W momencie złożenia wniosku o dofinansowanie kosztów nauki osoby niepełnosprawnej w ramach programu PFRON przetwarzane są następujące dane osobowe w formie papierowej:
- imię (imiona) i nazwisko wnioskodawcy;
- data urodzenia wnioskodawcy;
- numer PESEL wnioskodawcy;
- płeć wnioskodawcy;
- seria i numer dowodu osobistego wnioskodawcy;
- miejsce zamieszkania wnioskodawcy;
- telefon kontaktowy wnioskodawcy;
- imię (imiona) i nazwisko ucznia;
- data urodzenia ucznia;
- numer PESEL ucznia;
- płeć ucznia;
- miejsce zamieszkania ucznia;
- stopień niepełnosprawności;
- orzeczenie o niepełnosprawności;

- rodzaj niepełnosprawności;
- nazwa i adres szkoły ucznia;
- oświadczenie o wysokości dochodów wnioskodawcy.

31. Na potrzeby wykonania wykazu pracowników szkół przetwarzane są następujące dane osobowe w formie papierowej oraz w programie Kadry Radix:
    - imię (imiona) i nazwisko;
    - adres zamieszkania;
    - telefon kontaktowy;
    - data i miejsce urodzenia;
    - numer PESEL;
    - numer NIP;
    - imiona rodziców;
    - podleganie służbie wojskowej;
    - posiadanie gospodarstwa rolnego;
    - warunki zatrudnienia;
    - wynagrodzenie;
    - historia przebiegu pracy;
    - wykształcenie
    - dane ubezpieczeniowe.

32. Na potrzeby wydania informacji o dochodach nauczyciela przetwarzane są następujące dane osobowe w formie papierowej:
    - imię (imiona) i nazwisko;
    - data urodzenia;
    - PESEL
    - adres zamieszkania;
    - dochody podatnika;
    - NIP.

33. Na potrzeby prowadzenia rejestru skarg i wniosków przetwarzane są następujące dane osobowe w formie papierowej:

    - data wpływu;
    - imię i nazwisko petenta;
    - adres petenta.

34. W ramach programu Baza Azbestowa elektronicznie oraz w formie papierowej przetwarzane są dane osobowe na potrzeby stworzenia rejestru wyrobów zawierających azbest:
    - imię (imiona) i nazwisko właściciela;
    - adres występowania wyrobu zawierającego azbest.

35. Na potrzeby prowadzenia rejestru korespondencji przychodzącej i wychodzącej przetwarzane są następujące dane osobowe w formie papierowej:

    - imię (imiona) i nazwisko;
    - adres zamieszkania.

36. Na potrzeby prowadzenia rejestru numeracji porządkowej przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- imię (imiona) i nazwisko właściciela;
- adres zamieszkania;
- numer ewidencyjny działki;
- numer posesji;
- miejsce położenia nieruchomości.

37. Na potrzeby prowadzenia rejestru sieci wodociągowych przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- numer posesji;
- numer działki.

38. Na potrzeby prowadzenia rejestru wycinki drzew i krzewów przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- adres działki;
- akt własności jako załącznik (imię i nazwisko, adres zamieszkania, imiona rodziców).

39. Na potrzeby prowadzenia rejestru dzierżaw przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- numer PESEL;
- numer i seria dowodu osobistego;
- powierzchnia gospodarstwa.

40. Na potrzeby prowadzenia rejestru decyzji zatwierdzających podział działek przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- numer i miejscowość położenia działki.

41. Na potrzeby prowadzenia rejestru zaświadczeń o pracy w gospodarstwie rolnym przetwarzane są następujące dane osobowe w formie papierowej:

- imię (imiona) i nazwisko;
- nazwisko rodowe;
- adres zamieszkania;
- data urodzenia
- PESEL;

- imiona rodziców.

42. Na potrzeby prowadzenia rejestru warunków zabudowy o znaczeniu lokalnym przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- numer geodezyjny działek;
- nazwa i adres wnioskodawcy.

43. Na potrzeby prowadzenia rejestru celu publicznego przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- nazwa wnioskodawcy;
- adres zamieszkania;
- numer ewidencyjny gruntów.

44. Na potrzeby prowadzenia ewidencji zamówień publicznych przetwarzane są następujące dane osobowe w formie papierowej i elektronicznej:

- nazwa i adres oferenta.

45. W ramach prowadzenia dokumentacji kasowej przetwarzane są następujące dane osobowe w formie papierowej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- NIP.

46. W ramach prowadzenia rejestru poświadczeń za zgodność z oryginałem przetwarzane są następujące dane osobowe w formie papierowej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- PESEL.

47. W ramach prowadzenia rejestru poświadczeń własnoręczności podpisu przetwarzane są następujące dane osobowe w formie papierowej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- PESEL

48. W ramach prowadzenia list osób biorących udział w badaniu profilaktycznym przetwarzane są następujące dane osobowe w formie papierowej:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- numer ewidencyjny PESEL;
- numer telefonu.

49. Na potrzeby sporządzania testamentów i prowadzenia ich ewidencji przetwarzane są następujące dane osobowe w formie papierowej:

- imię i nazwisko spadkodawcy;
- imię i nazwisko świadków;
- adresy zamieszkania;
- stan majątkowy;
- seria i numer dowodu osobistego;
- data urodzenia.

50. Na potrzeby przewozu osób niepełnosprawnych samochodem służbowym przetwarzane są następujące dane osobowe w formie papierowej:

- imię i nazwisko;
- data i miejsce urodzenia;
- PESEL;
- rodzaj i numer dokumentu tożsamości;
- adres zamieszkania;
- orzeczenie o niepełnosprawności.

51. Na potrzeby prowadzenia rejestru zaświadczeń o przeznaczeniu gruntów przetwarzane są następujące dane osobowe:

- imię (imiona) i nazwisko;
- adres zamieszkania;
- numery działek.

52. Na potrzeby prowadzenia rejestru opłat skarbowych przetwarzane są następujące dane osobowe w formie elektronicznej w systemie DON (dziennik opłat nieprzypisanych):

- imię (imiona) i nazwisko;
- adres zamieszkania;

7. Sposób przepływu danych pomiędzy poszczególnymi systemami

System / Moduł „A”	System / Moduł „B”	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
PFRON	PFRON (serwer)	A do B	Poczta / Elektronicznie
Płatnik (baza pracowników urzędu i jednostek organizacyjnych)	ZUS	A do B	Internet
Płatnik (baza nauczycieli i pracowników szkół)	ZUS	A do B	Internet
Radix Kadry (baza pracowników urzędu i jednostek organizacyjnych)	Radix Płace (baza pracowników urzędu i jednostek organizacyjnych)	A do B	Elektroniczne
Radix Kadry (baza nauczycieli i pracowników szkół)	Radix Płace (baza nauczycieli i pracowników szkół)	A do B	Elektronicznie
Radix Płace (baza pracowników urzędu i jednostek organizacyjnych)	Urząd Skarbowy	A do B	Poczta
Radix Płace (baza pracowników urzędu i jednostek organizacyjnych)	Płatnik (baza pracowników urzędu i jednostek organizacyjnych)	A do B	Manualnie
Radix Płace (baza nauczycieli i pracowników szkół)	Płatnik (baza nauczycieli i pracowników szkół)	A do B	Elektronicznie
Radix Płace (baza nauczycieli i pracowników szkół)	Urząd Skarbowy	A do B	Poczta
Radix Płace (baza nauczycieli i pracowników szkół)	Bank	A do B	Poczta
Radix Pogrun	Radix WIP	A do B	Elektronicznie
Radix ELUD	Radix Pogrun	A do B	Elektronicznie
Radix ELUD	Radix WIP	A do B	Elektronicznie
Radix ELUD	Ośrodek Informatyki w Poznaniu	A do B	Poczta
Radix ELUD	PESEL MSWiA	A do B	Internet
Radix ELUD	Urząd Skarbowy	A do B	Poczta

Podmioty do których przekazywane są dane to:

- Zakład Ubezpieczeń Społecznych
- Powszechny Zakład Ubezpieczeń
- Urząd Skarbowy
- Podmioty zewnętrzne na podstawie odrębnych umów

Podmiotom powyższym dane te są przesyłane teletransmisyjnie lub w formie tradycyjnej za pośrednictwem Internetu i/lub poczt elektronicznych, mogą także być przekazywane na nośnikach danych takich jak np.: płyty CD. Przy użyciu Internetu realizowane są także przelewy bankowe i międzybankowe.

W związku z tym, iż w Urzędzie Gminy w Olszówce, dane osobowe przetwarzane są w komputerach posiadających połączenie z siecią publiczną (Internetem) stosowane są środki bezpieczeństwa na poziomie wysokim.

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

A. Środki ochrony fizycznej

1. Podstawowe zabezpieczenia fizyczne opisane są w Załączniku A „Wykaz zbiorów danych osobowych".
2. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
3. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
4. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej ogniotrwałej szafie metalowej

B. Środki sprzętowe, informatyczne i telekomunikacyjne

1. Pomieszczenia, w którym przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy.
2. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
3. Zbiór danych osobowych prowadzony jest przy użyciu komputera stacjonarnego i jest zabezpieczony poprzez indywidualny login i hasło.
4. Co najmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.
5. Lokalizacja urządzeń komputerowych (komputerów typu PC, drukarek itp.) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych.
6. Komputery przenośne, wykorzystywane do przetwarzania danych osobowych, po zakończonej pracy są przechowywane w warunkach zapewniających ich bezpieczeństwo.
7. System operacyjny zapewnia odpowiednie restrykcje w zakresie dostępu do danych i aplikacji.

8. Uniemożliwiono użytkownikom systemu informatycznego, w którym przetwarzane są dane osobowe wykonywania kopii tych danych.
9. Zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed awarią zasilania.
10. Zastosowano macierz dyskową w serwerze głównym w celu ochrony danych osobowych.
11. Użyto urządzenia UTM z wbudowanym Firewall'em, modułem IDS oraz IPS do ochrony dostępu do sieci komputerowej.

C. Środki ochrony w ramach oprogramowania urządzeń teletransmisji
1. Proces teletransmisji zabezpieczony jest za pomocą środków uwierzytelnienia.
2. Proces teletransmisji zabezpieczony jest za pomocą środków kryptograficznej ochrony danych osobowych.

D. Środki ochrony w ramach oprogramowania systemu
1. Dostęp do zbioru danych osobowych przetwarzanych za pomocą komputera zabezpieczony jest za pomocą hasła BIOS.
2. W systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł.
3. W systemie operacyjnym istnieją tylko konta domenowe.
4. Serwery obsługujące bazę danych oraz stanowiska komputerowe służące do przetwarzania danych osobowych dostępne są wyłącznie po przeprowadzeniu prawidłowego procesu autoryzacji (system użytkowników i haseł, ograniczenie dostępu do poziomu poleceń systemowych lub zakaz wykonywania poleceń systemowych.
5. Zapewniono rejestrację czasu nieudanych logowań do systemu przetwarzającego dane osobowe.
6. Zastosowano system rejestracji dostępu do zbioru danych osobowych.
7. Zastosowano oprogramowanie umożliwiające wykonanie kopii zapasowych zbiorów danych osobowych.
8. Zastosowano oprogramowanie zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego.

E. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych
1. Dostęp do zbioru danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano mechanizm umożliwiający rejestrację identyfikatora użytkownika wprowadzającego dane osobowe.
3. Wykorzystano środki pozwalające na rejestrację dokonanych zmian w zbiorze danych osobowych.
4. Zastosowano środki umożliwiające określenie praw dostępu do zbioru danych osobowych.
5. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
6. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.
7. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

F. Środki ochrony w ramach systemu operacyjnego

1. Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku nieaktywności użytkownika dłuższej niż 15 minut.
2. Zastosowano działający w tle program antywirusowy na komputerach użytkowników.

G. Środki organizacyjne

1. Powołano Administratora Bezpieczeństwa Informacji w osobie Pani Elwir Nity.
2. Opracowano i wdrożono Politykę bezpieczeństwa informacji oraz Instrukcję zarządzania systemem informatycznym.
3. Wdrożono odpowiedni podział obowiązków i kontroli dostępu.
4. Do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.
5. Administrator Danych Osobowych prowadzi Ewidencję osób upoważnionych do przetwarzania danych osobowych.
6. Wprowadzono mechanizmy autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich.
7. Wprowadzono procedury alarmowe i informacyjne.
8. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia.
9. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy.
10. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
11. Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarce.
12. Zapewniono klauzule poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych w Urzędzie Gminy w Olszówce.
13. Zapewnia się bezpieczne przechowywanie lub niszczenie uszkodzonych nośników zawierających dane osobowe (np. dysk twardy), szczególnie, gdy sprzęt, w którym zamontowany jest dany nośnik przekazywany jest do naprawy do firmy zewnętrznej.

9. Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

9.1. Zdarzenia zagrażające bezpieczeństwu danych osobowych

Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:

1. próby naruszenia ochrony danych:
   - z zewnątrz – włamania do systemu, podsłuch, kradzież danych,
   - z wewnątrz – nieumyślna lub celowa modyfikacja danych, kradzież danych,
2. programy destrukcyjne:
   - wirusy,
   - konie trojańskie,
   - makra,
   - bomby logiczne,
3. awarie sprzętu lub uszkodzenie oprogramowania,
4. utrata sprzętu lub nośników z ważnymi danymi,
5. inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych.
6. usiłowanie zakłócenia działania systemu informatycznego,

9.2. Procedura postępowania w przypadkach naruszenia bezpieczeństwa danych osobowych

1. W przypadku stwierdzenia faktu nieuprawnionego przetwarzania, ujawnienia lub nienależytego zabezpieczenia przed osobami nieuprawnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych, każdy pracownik Urzędu Gminy w Olszówce zobowiązany jest poinformować bezpośredniego przełożonego, który powiadamia o zdarzeniu Administratora Bezpieczeństwa Informacji, a ten Wójta Gminy Olszówka.
2. W sytuacji, określonej w pkt. 1, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
   - ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   - ustala osoby odpowiedzialne za naruszenie,
   - podejmuje działania w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości,
   - sporządza pisemną notatkę z przeprowadzonego postępowania.
3. Administrator Bezpieczeństwa Informacji powiadamia o wynikach postępowania wyjaśniającego Wójta Gminy Olszówka.
4. W przypadku zaistnienia zdarzenia, określonego w ust. 1, decyzje dyscyplinarne w stosunku do winnych oraz w sprawie wniosku o pociągnięcie ich do odpowiedzialności karnej podejmuje Wójt Gminy Olszówka z własnej inicjatywy lub na wniosek Administratora Bezpieczeństwa Informacji.

9.3. Procedura postępowania w przypadkach zagrożeń

1. W przypadku jakiejkolwiek nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia o uszkodzenie sprzętu, oprogramowania lub danych należy bezzwłocznie powiadomić administratora systemu, bezpośredniego przełożonego, który zawiadamia Administratora Bezpieczeństwa Informacji.
2. W przypadku włamania lub podejrzenia o włamanie do systemu administrator danego systemu podejmuje działania w celu zabezpieczenia systemu i danych:
    - zmienia hasła administracyjne,
    - określa rodzaj i sposób włamania,
    - podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu,
    - szacuje straty w systemie,
    - przywraca stan systemu sprzed włamania.
3. W przypadku uszkodzenia sprzętu lub programów z danymi administrator danego systemu podejmuje działania w celu:

- określenia przyczyny uszkodzenia,
- oszacowania strat wynikłych z w/w uszkodzenia,
- naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego zainstalowania danego programu, odtworzenie jego pełnej konfiguracji oraz wczytania danych z ostatniej kopii zapasowej.

4. W przypadku uszkodzenia danych administrator systemu podejmuje następujące działania:

- ustala przyczynę uszkodzenia danych,
- określa wielkość i jakość uszkodzonych danych,
- podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej.

5. W przypadku stwierdzenia nieprawidłowości w funkcjonowaniu sieci telekomunikacyjnej każdy użytkownik zobowiązany jest niezwłocznie powiadomić administratora sieci, który podejmuje działania w celu ustalenia przyczyn zaistniałej sytuacji oraz wyeliminowania nieprawidłowości.

W przypadku zidentyfikowania osób odpowiedzialnych za wystąpienie któregoś ze zdarzeń zagrażających bezpieczeństwu danych administrator danego systemu zobowiązany jest powiadomić bezpośredniego przełożonego winnej osoby oraz Administratora Bezpieczeństwa Informacji, a ten Wójta Gminy Olszówka.

10. Procedura działań korygujących i zapobiegawczych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub słabości systemu ochrony danych osobowych.
2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa, zagrożenia lub słabości systemu ochrony danych osobowych mogą wpłynąć na zgodność z wymaganiami stawy o Ochronie Danych Osobowych, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji. Przy czym czynności związane z realizacją poszczególnych zadań / zabezpieczeń wykonuje osoba odpowiedzialna a zatwierdza Wójt Gminy Olszówka.

Definicje:

1. Niezgodność – niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
2. Incydent – naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
3. Zagrożenie – potencjalna możliwość wystąpienia incydentu
4. Słabość systemu – zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu
5. Działanie korygujące – jest to działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności / incydentu lub innej niepożądanej sytuacji.
6. Działanie zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności / incydentu lub innej potencjalnej sytuacji niepożądanej.
7. Korekcja – działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.
8. Kontrola (Audyt) – systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań, polityk i procedur.

Opis czynności:

1. ABI jest odpowiedzialny za analizę incydentów bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:

- zgłoszenia od pracowników
- alarmy z systemów informatycznych
- analizy incydentów
- wyniki audytów / kontroli

2. Gdy ABI stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:

- Źródło powstania incydentu / zagrożenia lub słabości
- Zakres działań korygujących lub zapobiegawczych
- Termin realizacji
- Osobę odpowiedzialną

3. ABI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, ABI jest zobowiązany do oceny efektywności ich zastosowania.
5. Powyższe czynności ABI powinien rejestrować w pliku „Raport z naruszenia bezpieczeństwa systemu informatycznego".

11. Kontrola systemu ochrony danych osobowych i przegląd zarządzania

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: kontrolą stanu bezpieczeństwa danych osobowych oraz okresową oceną Systemu Ochrony Danych Osobowych
2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
3. Do kontroli stanu ochrony danych osobowych w Urzędzie Gminy w Olszówce upoważnieni są:
   - Wójt Urzędu Gminy w Olszówce lub osoby przez niego upoważnione,
   - Administrator Bezpieczeństwa Informacji.
4. Raz w roku kontroli (audytowi) podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.
5. Administrator Bezpieczeństwa Informacji przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe.
6. Kontroli podlega warstwa sprzętowa, systemy operacyjne oraz aplikacje, realizacja zabezpieczeń przez pracowników firmy i przestrzeganie polityki bezpieczeństwa.
7. Po dokonanej kontroli Administrator Bezpieczeństwa Informacji przygotowuje raport poaudytowy. Na jego podstawie informuje Wójta Urzędu Gminy w Olszówce o konieczności podjęcia właściwych działań korygujących i doskonalących.
8. Raz w roku po przeprowadzonej kontroli Administrator Bezpieczeństwa Informacji przygotowuje ocenę roczną stanu funkcjonowania systemu ochrony danych osobowych i przedstawia go Wójtowi Urzędu Gminy w Olszówce na Przeglądzie zarządzania ODO. Na jej podstawie informuje Wójta Urzędu Gminy w Olszówce o konieczności podjęcia właściwych działań korygujących i doskonalących. Potwierdzeniem przeprowadzenia przeglądu zarządzania ODO jest odpowiedni protokół stworzony przez Administratora Bezpieczeństwa Informacji.

12. Postanowienia końcowe

1. „Polityka Bezpieczeństwa" jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Wójt Urzędu Gminy w Olszówce jest zobowiązany do zapoznania z treścią „Polityki bezpieczeństwa informacji" każdego użytkownika.
3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
4. Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika.
   - Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
   - Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
   - Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
5. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce".
6. W sprawach nieuregulowanych w niniejszej „Polityce bezpieczeństwa informacji" mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tj. Dz. U. z 2002r., Nr 101, poz. 926 ze zm.) oraz wydanych na jej podstawie aktów wykonawczych.

Załącznik Nr 2
do Zarządzenia Nr 9/2010
Wójta Gminy Olszówka
z dnia 01.10.2010 r.

Instrukcja określająca sposób zarządzania systemem informatycznym Urzędu Gminy w Olszówce

Spis treści

1. Wstęp

Instrukcja stanowi zestaw procedur opisujących zasady zapewnienia bezpieczeństwa danych osobowych w systemach i aplikacjach informatycznych.

2. Definicje

ASI – Administrator Systemu Informatycznego
ABI – Administrator Bezpieczeństwa Informacji

3. Poziom bezpieczeństwa

W Urzędzie Gminy w Olszówce obowiązuje wysoki poziom bezpieczeństwa systemu informatycznego.

4. Bezpieczna eksploatacja sprzętu i oprogramowania

Celem procedury jest określenie wymagań bezpieczeństwa dla sprzętu i oprogramowania eksploatowanego w Urzędzie Gminy w Olszówce.

1. Sprzęt służący do przetwarzania zbioru danych osobowych składa się z: komputerów stacjonarnych klasy PC, notebooków oraz serwerów.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.
3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
4. Sieć komputerowa służąca do przetwarzania danych osobowych posiada zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
5. Główne węzły są podtrzymywane przez UPS zapewniający odpowiedni czas pracy systemu.
6. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
7. ASI odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.
8. Ekrany monitorów są wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
9. Ekrany monitorów, są ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

10. Za spełnienie obowiązku określonego w powyższym rozdziale odpowiadają użytkownicy:
    - Włodzimierz Fraszczyk
    - Elżbieta Wieczorek
    - Elwira Nita
    - Elżbieta Michalak
    - Elżbieta Banasiak
    - Karol Maluga
    - Rafał Ławniczak
    - Ewa Wawrzyniak
    - Sylwia Sulińska
    - Maria Siwińska
    - Agnieszka Sawicka
    - Barbara Wotalska
    - Agnieszka Maluga
    - Bożena Czubaszewska
    - Ewa Nowińska
    - Katarzyna Leń
    - Piotr Łoboda
    - Emilia Marciniak
    - Aleksandra Lasota

5. Procedura dostępu podmiotów zewnętrznych

Celem procedury jest zapewnienie bezpiecznej współpracy z podmiotami zewnętrznymi, ponieważ dostęp podmiotów zewnętrznych (osób fizycznych lub prawnych) do systemu informatycznego Urzędu Gminy w Olszówce i danych osobowych wiąże się zarówno z ryzykiem nie zapewnienia właściwej ochrony informacjom, jak również z pozyskaniem informacji nieprzeznaczonych dla tej osoby.

1. Podmiot zewnętrzny mający dostęp do systemu informatycznego i danych osobowych administrowanych przez Urząd Gminy w Olszówce powinien posiadać klauzulę o poufności w umowie o współpracy.
2. Podmiot zewnętrzny jest zobowiązany do zapewnienia ochrony danych osobowych pozyskanych lub udostępnionych mu przy / lub w związku z wykonywaniem umowy, na zasadach wynikających z obowiązujących przepisów prawa oraz polityk, instrukcji lub innych regulacji o charakterze wewnętrznym w tym przedmiocie, obowiązujących w Urzędzie Gminy w Olszówce.
3. Dostęp do danych osobowych, przetwarzanie lub usuwanie tych danych, administrowanych przez Urząd Gminy w Olszówce, wymaga odrębnego upoważnienia. Uprawnienia lub czynności te mogą być przyznane lub wykonywane wyłącznie dla celów związanych z wykonywaniem umowy i wyłącznie na/lub w okresie niezbędnym dla realizacji tych celów.
4. Tworzenie przez podmiot zewnętrzny zbiorów danych osobowych wykorzystujących dane administrowane przez Urząd Gminy w Olszówce wymaga każdorazowo pisemnej zgody Wójta Gminy Olszówka.
5. Urządzenia i systemy informatyczne podmiotu zewnętrznego, na których będą przetwarzane dane osobowe, pozyskane lub udostępnione w związku

z wykonywaniem umowy, winny spełniać wymagania techniczne odpowiednie dla urządzeń służących do przetwarzania danych osobowych.

6. Podmiot zewnętrzny ponosi odpowiedzialność za będące następstwem jego zachowań szkody wyrządzone niezgodnym z umową przetwarzaniem danych osobowych, w szczególności szkody wyrządzone utratą, niewłaściwym przechowywaniem lub posłużeniem się dokumentami, które są nośnikiem danych osobowych.
7. W przypadku, gdy umowa z podmiotem zewnętrznym uprawnia do jej wykonywania przy udziale osób trzecich, postanowienia paragrafów poprzedzających rozciągają się również na te osoby, przy czym podmiot zewnętrzny odpowiada za działania lub zaniechania osób, którymi się posługuje, lub którym powierza wykonanie niniejszej umowy, jak za działania lub zaniechania własne.
8. Administrator Bezpieczeństwa Informacji prowadzi rejestr podmiotów zewnętrznych posiadających dostęp do systemu informatycznego Urzędu Gminy w Olszówce i danych osobowych celem identyfikacji i zapewnienia Urzędowi Gminy w Olszówce nadzoru nad bezpiecznym ich przetwarzaniem. Patrz Załącznik nr 4 – Rejestr podmiotów zewnętrznych.

6. Procedura korzystania z Internetu i poczty elektronicznej

Celem procedury jest uregulowanie zasad korzystania z Internetu i poczty elektronicznej, aby zagwarantować bezpieczeństwo danych osobowych przesyłanych przez te media.

Użytkownicy Internetu zobowiązani są do przestrzegania następujących zasad:

1. Zakazuje się ściągania przez użytkowników plików lub przeglądania zasobów informacyjnych o treści prawnie zabronionej, obscenicznej bądź pornograficznej.
2. Zaleca się, aby do wymiany korespondencji w czasie korzystania z systemu informatycznego firmy powinna być wykorzystywana służbowa poczta elektroniczna.
3. Szczególne rygory należy stosować wobec ściągania z Internetu plików wykonywalnych. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora Bezpieczeństwa Informacji i tylko w uzasadnionych przypadkach. Informatyk może nakazać przetestowanie ściągniętego oprogramowania w odseparowanym środowisku. Za przeprowadzenie testów odpowiada użytkownik, ich wyniki powinny zostać przekazane Administratorowi Bezpieczeństwa Informacji oraz ASI. Po ich zaakceptowaniu użytkownik może dokonać instalacji oprogramowania. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane.
4. Do korzystania z Internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez Administratora Bezpieczeństwa Informacji formy dostępu. W szczególności zabrania się łączenia się użytkowników systemu informatycznego Urzędu Gminy w Olszówce poprzez łącza komutowane, jeżeli można skorzystać z centralnego punktu dostępu do Internetu.
5. ABI stosuje mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one:
    - Blokowanie stron internetowych określonego typu,
    - Blokowanie określonych stron internetowych,
    - Analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

Użytkownicy systemu poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:

1. Przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z Administratorem Bezpieczeństwa Informacji.
2. Przesyłanie informacji poza obręb Urzędu Gminy w Olszówce może odbywać się tylko przez osoby do tego upoważnione.
3. Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. W przypadku przesyłania informacji wrażliwych wewnątrz Urzędu Gminy w Olszówce bądź informacji wewnętrznych poza Urząd należy wykorzystywać mechanizmy kryptograficzne.
5. Jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją. Adresat zobowiązany jest w takiej sytuacji przesłać nadawcy potwierdzenie.
6. Informacje przesyłane za pośrednictwem poczty elektronicznej muszą być zgodne z prawem i z zasadami obowiązującymi w przedsiębiorstwie.
7. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej przesyłki, użytkownik powinien ją zniszczyć lub skontaktować się z Administratorem Bezpieczeństwa Informacji.
8. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu Administratora Bezpieczeństwa Informacji, który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji.
9. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia" itp.
10. Użytkownicy nie powinni rozsyłać, wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów – określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej.
11. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

7. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest zapewnienie użytkownikom odpowiednich uprawnień do przetwarzania danych osobowych, aby redukować zagrożenie nieuprawnionego dostępu do danych osobowych i utraty poufności.

A. Podstawowe zasady nadawania uprawnień w systemie

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każdy pracownik Urzędu Gminy w Olszówce powinien zostać zapoznany przez bezpośredniego przełożonego lub Administratora Bezpieczeństwa Informacji z przepisami dotyczącymi ochrony danych osobowych, a na dowód przeszkolenia

złożyć stosowne oświadczenie u Administratora Bezpieczeństwa Informacji. Wzór oświadczenia określa Załącznik nr 1.

2. Dział Kadr Urzędu Gminy w Olszówce zobowiązany jest do włączenia do indywidualnych zakresów obowiązków służbowych każdego pracownika zatrudnionego przy przetwarzaniu danych osobowych – obowiązku ochrony danych osobowych oraz odpowiedzialności za nieuzasadnioną ich modyfikację lub zniszczenie bądź nielegalne ujawnienie lub pozyskanie.

B. Procedura nadawania uprawnień do przetwarzania danych osobowych

1. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienia wydane przez Administratora Bezpieczeństwa Informacji.
2. Dostęp do pomieszczenia, w którym znajduje się serwer oraz urządzenia wchodzące w jego skład mają tylko osoby posiadające upoważnienie – Załącznik nr 2.
3. Procedury wydawania i anulowania upoważnień do obsługi systemu informatycznego oraz nadawania, modyfikacji i anulowania uprawnień użytkowników do systemu realizowane są wg następujących zasad:
    a) Pracownicy Urzędu Gminy w Olszówce składają do ABI wniosek o upoważnienie do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych.
    b) ABI wydaje wnioskowane Upoważnienie, a następnie przekazując go Administratorowi Systemu Informatycznego – zleca zarejestrowanie użytkownika w systemie informatycznym oraz nadanie mu indywidualnego identyfikatora. Wzór „Upoważnienia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych". Wzór Wniosku określa Załącznik nr 3.
    c) Administrator Systemu Informatycznego, po otrzymaniu określonego dokumentu rejestruje użytkownika w systemie nadając mu identyfikator i wnioskowane uprawnienia oraz zwraca ABI wypełnione Zlecenie;
    d) Oryginał Upoważnienia pozostaje u ABI, a jego kopia zostaje przekazana osobie, dla której upoważnienie zostało wydane, oraz kierownikowi właściwej jednostki lub komórki organizacyjnej (część Upoważnienia niezawierająca identyfikatora użytkownika);
    e) W przypadku zmiany przez użytkownika uprawnień do obsługi danego systemu, ABI Urzędu Gminy w Olszówce zleca Administratorowi Systemu Informatycznego modyfikację uprawnień;
    f) W przypadku utraty przez użytkownika uprawnień do obsługi danego systemu informatycznego (np. rozwiązanie stosunku pracy, nieobsługiwanie systemu z powodu zmiany stanowiska pracy) ABI występuje do Administratora Systemu Informatycznego z wnioskiem o anulowanie upoważnienia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, zgodnie z Załącznikiem nr 3;
    g) ABI zleca Administratorowi Systemu Informatycznego wyrejestrowanie użytkownika z systemu (zablokowanie dostępu do systemu), przekazując mu wydane „Upoważnienie / anulowanie upoważnienia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych", którego wzór przedstawia Załącznik nr 3;

h) Administrator Systemu Informatycznego, po otrzymaniu określonego dokumentu wyrejestrowuje użytkownika z systemu (blokuje jego dostęp do systemu) oraz zwraca ABI wypełnione Anulowanie upoważnienia;
i) Oryginał Anulowania upoważnienia pozostaje u ABI, a kopie zostają przekazane Administratorowi Systemu Informatycznego oraz osobie, której upoważnienie zostało anulowane.

4. Identyfikator użytkownika nadany na podstawie wniosku „Zlecenia nadania zmiany anulowania zakresu uprawnień użytkownika", wraz z imieniem i nazwiskiem właściciela identyfikatora, ABI wpisuje do „Ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych", zgodnie z Załącznikiem 5.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

8. Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

Zasady ogólne

1. Pierwsze hasło dla użytkownika ustala przydziela ASI przy wprowadzaniu identyfikatora użytkownika do systemu.
2. Użytkownik systemu niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ASI.
3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło dostępu.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Hasło nie może być ujawnione nawet po utracie przez nie ważności.
6. Hasła mają charakter poufny – są znane tylko jego właścicielowi.
7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
8. Hasła w bazie są zapisywane w systemie w postaci szyfrowanej.
9. Osobą odpowiedzialną za przydział haseł i częstotliwość ich zmiany, a także w zakresie rejestrowania i wyrejestrowania użytkowników jest Administrator Systemu Informatycznego. Wyznacza się jako: Administratora Systemu Informatycznego w Urzędzie Gminy w Olszówce Pana Piotra Łobodę W razie nieobecności Administratora Systemu zastępstwo obejmuje Pani Elwira Nita.

Hasła administratora

1. Administrator systemu 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 spisanie oraz umieszczenie 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.

Uwierzytelnianie na poziomie systemu operacyjnego

1. Hasło na poziomie dostępu do systemu operacyjnego musi składać się z co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasło musi być różne od trzech ostatnio używanych.
3. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.
4. Zmiana hasła do systemu operacyjnego następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

Uwierzytelnianie na poziomie dostępu do aplikacji

1. Hasło na poziomie dostępu do aplikacji w której przetwarza się dane osobowe musi składać się z co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasło musi być różne od trzech ostatnio używanych
3. Za systematyczną, terminową zmianę hasła odpowiada ASI.
4. Zmiana hasła do systemu operacyjnego następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

9. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia użytkownika.
3. Jeśli system to umożliwia, po przekroczeniu 3 prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.
4. ASI ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną.
5. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:
   a) wylogować się z systemu informatycznego lub,
   b) wywołać blokowany hasłem wygaszacz ekranu.
6. Kończąc pracę należy:

a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

10. Procedura tworzenia kopii zapasowych

Tworzenie kopii bezpieczeństwa baz danych programów, w których są przetwarzane dane osobowe

1. Bazy danych programów w których są przetwarzane dane osobowe są umieszczone na centralnym serwerze wyposażonym w technologię RAID 5.
2. W skład wszystkich kopii zapasowych wchodzą bazy danych programów, dokumenty wspólne użytkowników oraz dokumenty indywidualne każdego z użytkowników.
3. Dzienne kopie zapasowe wykonywane są z wykorzystaniem technologii taśmowej. Każdy kopia dzienna przechowywana jest na oddzielnej taśmie przypisanej do konkretnego dnia.
4. Miesięczna kopia zapasowa przechowywana jest na sieciowej macierzy dyskowej.
5. Raz w miesiącu tworzona jest dodatkowa miesięczna kopia zapasowa, która jest nagrywana na nośnikach DVD.
6. Kopie zapasowe są odpowiednio oznaczone.
7. Kopie zapasowe są przychowane w szafie pancernej.
8. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
9. W przypadku wystąpienia problemów z archiwizacją, konieczny jest kontakt z ASI.

11. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

Procedura określa sposób postępowania z nośnikami, na których znajdują się dane osobowe, celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

A. Elektroniczne nośniki informacji

1. Pracownicy nie mogą wynosić na zewnątrz Urzędu Gminy w Olszówce wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Wójta Urzędu Gminy w Olszówce.
2. Dane osobowe w postaci elektronicznej należy usuwać z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie niezwłocznie, po wykorzystaniu tych danych chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
3. Uszkodzone nośniki komputerowe, zawierające dane osobowe, są fizycznie niszczone przy udziale komisji powołanej przez Wójta Gminy Olszówka, która wykonuje czynności na podstawie instrukcji w/g Załącznika nr 6.

4. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
5. Przekazywanie nośników z danymi osobowymi jest przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji Administratora Bezpieczeństwa Informacji.
6. Zaleca się, aby informacje wewnętrzne znajdujące się na nośnikach przenośnych, wynoszonych poza teren Urzędu Gminy w Olszówce, były szyfrowane.

B. Kopie zapasowe

1. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w szafie pancernej znajdującej się w pomieszczeniu sekretariatu Urzędu Gminy w Olszówce.
2. Dostęp do kopii zapasowych mają tylko upoważnieni pracownicy, tj. ABI oraz ASI.
3. Kopie bezpieczeństwa przechowywane są przez okres 12 miesięcy.
4. Kopie archiwalne miesięczne przechowywane są przez okres 1 roku, a kopie roczne przez 5 lat, licząc od pierwszego dnia roku następującego po roku, za który wykonana jest kopia.
5. Nośniki, na których znajdują się kopie zawierające dane osobowe, są oznaczone w sposób trwały, jednoznaczny i czytelny i zaewidencjonowane w „Rejestrze nośników zawierających dane osobowe" stanowiącym Załącznik nr 7 do niniejszej Instrukcji.
6. Kopie archiwalne należy:
    - okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania,
    - bezzwłocznie usuwać po ustaniu ich użyteczności.

C. Wydruki

1. Wydruki/dokumenty, zawierające dane osobowe, przechowuje się w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa według Załącznika 8
2. Wydruki/dokumenty, zawierające dane osobowe, należy niszczyć przez pocięcie w niszczarce.
3. Za bezpieczeństwo danych osobowych zapisanych w formie papierowej odpowiedzialne są osoby je przetwarzające oraz Administrator Bezpieczeństwa Informacji.

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

A. Ochrona antywirusowa

1. Za ochronę antywirusową odpowiada ASI.
2. System antywirusowy działa centralnie.
3. System antywirusowy zainstalowany jest na każdym komputerze z dostępem do danych.
4. Programy antywirusowe, o których mowa poprzednio, winny być uaktywnione cały czas podczas pracy danego systemu.
5. 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.
6. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.

B. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

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

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

1. 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 w Olszówce,
   c) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
   d) podmiotu, któremu powierzono przetwarzanie danych,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
2. Dane osobowe administrowane przez Urząd Gminy w Olszówce mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy Ustawy o Ochronie Danych Osobowych oraz innych przepisów powszechnie obowiązujących.

3. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.
4. Dane udostępnione Urzędowi Gminy w Olszówce przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. ABI prowadzi ewidencję udostępniania danych, o których mowa w pkt. 2. Jest ona przedstawiona jako Załącznik 4.
6. Odnotowanie obejmuje informacje o:
    a) Nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
    b) Zakresie udostępnianych danych,
    c) Dacie udostępnienia,
7. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
8. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w pisemnym raporcie i przekazywane tej osobie.

14. Procedura wykonywania przeglądów i konserwacji

1. Przeglądy i konserwacja systemu informatycznego powinny być wykonywane w terminach określonym przez producentów systemu oraz zgodnie z harmonogramem ASI
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 ASI.
4. Nieprawidłowości w działaniach systemu informatycznego oraz oprogramowania powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.
5. 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
6. 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.