Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji

Z

Polityką Bezpieczeństwa Systemu Teleinformacyjnego

Urzędu Gminy w Wilkowicach

Spis treści

I Rozdział

Polityka Bezpieczeństwa

I.1 Deklaracja Urzędu Gminy Wilkowice

Mając świadomość znaczenia informacji i systemów informacyjnych dla realizacji misji i celów Urzędu Gminy Wilkowice. zapewniam, że podejmowane przez Urząd działania dążą do zapewnienia bezpieczeństwa zasobów informacyjnych i są zgodne z wymogami obowiązującego prawa oraz normą PN EN ISO 27000 jako podstawy do realizacji zadań zapewnienia bezpieczeństwa w urzędzie

W celu udokumentowania realizacji Zarządzania Bezpieczeństwem Informacji przyjmuję Politykę Bezpieczeństwa Systemu Informacyjnego.

Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w dokumentach Polityki Bezpieczeństwa Systemu Informacyjnego obowiązują wszystkich pracowników Urzędu.

Funkcjonujący System Zarządzania Bezpieczeństwem Informacji jest w pełni zgodny z wymaganiami obowiązującego prawa oraz zdąża do zasad ujętych w normie PN EN ISO 27000 i będzie nieustannie nadzorowany i doskonalony.

Wójt Gminy

WÓJT

Mieczysław Rączka

I.2 Polityka Bezpieczeństwa Danych przetwarzanych w systemie informatycznym

Celem niniejszej polityki jest określenie podstawowych zasad bezpiecznego przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy Wilkowice. Wszelkie dokumenty określające zasady przetwarzania danych osobowych w systemie informatycznym winny być zgodne z niniejszą polityką.

Polityka ta została opracowana i wdrożona ze względu na fakt, iż Urząd Gminy Wilkowice jest administratorem danych osobowych, w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. nr 101 poz. 926 z późn. zm.) zwana dalej „ustawą". Niniejsza polityka dotyczy wszystkich osób biorących udział w sposób bezpośredni lub pośredni w przetwarzaniu danych, w tym osobowych w systemie informatycznym w urzędzie.

Polityka niniejsza jest zgodna ze stanem prawnym na dzień 1 czerwca 2007 r.

Wójt Urzędu Gminy Wilkowice, rozumiejąc konieczność zabezpieczenia danych, w tym osobowych przetwarzanych w systemie informatycznym urzędu wynikającą z obowiązujących w Polsce przepisów prawa, deklaruje pełne wsparcie dla podejmowanych działań uzasadnionych realizacją celów zabezpieczenia danych, w tym osobowych przetwarzanych w systemie informatycznym.

Wójt Urzędu Gminy Wilkowice, pełniąc rolę Administratora Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji w celu sprawowania nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa danych osobowych, koordynacji procesów związanych z zarządzaniem systemem informatycznym przetwarzającym dane osobowe w aspekcie ich bezpieczeństwa oraz bezpośredniego reprezentowania go wobec Administratora Systemu Informatycznego.

Wszystkie osoby biorące bezpośredni lub pośredni udział w procesie przetwarzania danych, w tym osobowych w systemie informatycznym, są odpowiedzialne za właściwe zabezpieczenie tych danych.

Zabezpieczenie danych, w tym osobowych przetwarzanych w systemie informatycznym, obejmuje:

- ochronę poufności rozumianej jako zabezpieczenie informacji przed dostępem do niej osób nieuprawnionych
- ochronę integralności rozumianej jako zabezpieczenie informacji przed wprowadzeniem przypadkowych lub celowych zmian powodujących jej zafałszowanie
- ochronę dostępności rozumianej jako zabezpieczenie informacji przed jej zniszczeniem, jak również zapewnienie takiego działania systemu informatycznego, aby dane osobowe były dostępne dla osób upoważnionych do ich przeglądania oraz przetwarzania.

Zabezpieczenia są określane na podstawie obowiązujących wymagań prawnych i wyników procesu analizy ryzyka. Za koordynację procesu analizy ryzyka odpowiedzialny jest Administrator Bezpieczeństwa Informacji, natomiast za jego wykonanie Administrator Systemów Informatycznych.

Przetwarzanie danych, w tym osobowych w systemach informatycznych, jest dopuszczalne pod warunkiem:

- spełnienia szczegółowych zaleceń dotyczących systemów informatycznych opisanych w niniejszej

polityce, jak również w dokumentach z nią związanych
- posiadania przez systemy informatyczne mechanizmów pozwalających na realizację procesów zabezpieczenia danych osobowych opisanych w niniejszej polityce, jak również w dokumentach z nią związanych
- przetwarzania danych osobowych w zakresie dopuszczalnym ze względu na zapisy Ustawy, w szczególności z uwzględnieniem zapisów art. 27 Ustawy.

Systemy informatyczne przetwarzające dane, w tym dane osobowe, umieszczone są w kontrolowanych przez odpowiedzialnego za dany sprzęt na którym są przetwarzane dane osobowe pracownika. Pracownicy upoważnieni i zarazem odpowiedzialni za ochronę danych przetwarzanych na będącym w ich użytkowaniu komputerze są zobowiązani do stosowania procedur wynikających z niniejszej instrukcji.

Dane, w tym dane osobowe, mogą być przetwarzane na komputerach przenośnych znajdujących się poza wyznaczoną strefą pod warunkiem zastosowania szczególnych warunków bezpieczeństwa określonych dla tego rodzaju urządzeń.

Dane, w tym dane osobowe, przetwarzane w systemie informatycznym i przesyłane za pośrednictwem sieci informatycznych powinny być zabezpieczone przy użyciu mechanizmów kryptograficznych, jeżeli wyniki analizy ryzyka wskazują na taką potrzebę.

Dostęp użytkowników do systemu informatycznego przetwarzającego dane, w tym dane osobowe, jest kontrolowany za pomocą mechanizmów uwierzytelnienia, autoryzacji i rozliczalności. Podstawą uwierzytelnienia użytkownika jest wykorzystanie unikalnego dla użytkownika identyfikatora i hasła. Autoryzacja użytkownika odbywa się na podstawie nadanych przez Administratora Bezpieczeństwa Informacji, a wprowadzonych przez Administratora Systemu Informatycznego zakresu indywidualnych uprawnień. System informatyczny przetwarzający dane, w tym dane osobowe, jest wyposażony w mechanizmy pozwalające w sposób jednoznaczny przypisać wykonanie określonych operacji na danych osobowych konkretnemu użytkownikowi. Rodzaje operacji i szczegółowość zapisu jest określana w oparciu o wyniki analizy ryzyka oraz obowiązujące regulacje prawne.

Wszelkiego rodzaju nośniki danych osobowych, które są przekazywane osobom lub podmiotom nieupoważnionym do otrzymania tych danych lub też gdy istnieje podejrzenie, że mogą się one znaleźć w rękach osób nieupoważnionych do otrzymania danych, w tym danych osobowych (na przykład w procesie likwidacji), pozbawia się danych lub też doprowadza do stanu uniemożliwiającego ich odczytanie. Za pozbawienie zapisu odpowiada osoba przekazująca nośnik lub odpowiadająca za realizację działań, w wyniku których nośnik może stać się dostępny dla osób nieupoważnionych do otrzymania danych osobowych.

W razie gdy przekazanie nośnika osobie nie będącej pracownikiem Urzędu Gminy Wilkowice jest związane z jego naprawą lub konserwacją albo naprawą lub konserwacją urządzenia, którego składową jest nośnik, dopuszczalne jest pozostawienie zapisanych danych pod warunkiem sprawowania nadzoru przez Administratora Bezpieczeństwa Informacji lub Systemu Informatycznego w trakcie trwania naprawy lub konserwacji.

Dane, w tym dane osobowe, są zabezpieczane przez tworzenie kopii awaryjnych. Za poprawność przebiegu procesu tworzenia kopii awaryjnych, jak również za bezpieczne składowanie nośników kopii i ich udostępnianie odpowiada Administrator Systemów Informatycznych. Za składowanie informacji w sposób umożliwiający wykonanie kopii, w szczególności na centralnych serwerach, odpowiadają użytkownicy systemu informatycznego.

Różnego rodzaju nośniki wszelkich danych, w tym również kopie zapasowe danych, w tym danych osobowych, muszą być przechowywane w sposób zapewniający odpowiednią - wynikającą z analizy ryzyka - ochronę przed dostępem do nich osób niepowołanych oraz przed celowym lub przypadkowym zniszczeniem, w tym również zniszczeniem wynikającym z warunków środowiskowych Urzędu Gminy Wilkowice. Za sporządzenie szczegółowych wytycznych w zakresie zabezpieczenia nośników danych osobowych odpowiada Administrator Systemów Informatycznych.

W wypadku wystąpienia przypadkowego lub celowego naruszenia bezpieczeństwa danych, w tym także danych osobowych, Administrator Systemów Informatycznych jest odpowiedzialny za przeprowadzenie procesu usuwania skutków naruszenia bezpieczeństwa danych osobowych z uwzględnieniem wykrycia przyczyn zaistnienia incydentu, przekazania Administratorowi Danych Osobowych oraz Administratorowi Bezpieczeństwa informacji o ewentualnych sprawcach oraz przeanalizowania możliwości wprowadzenia zabezpieczeń redukujących ryzyko wystąpienia w przyszłości podobnego incydentu.

Każda osoba, która zauważy naruszenie bezpieczeństwa danych osobowych, a w szczególności:

- ujawnienie lub możliwość ujawnienia danych osobowych osobom nieupoważnionym
- zafałszowanie danych osobowych lub możliwość wystąpienia zafałszowania danych osobowych
- zniszczenie lub możliwość zniszczenia danych osobowych
- zablokowanie lub możliwość zablokowania pracy systemu informatycznego przetwarzającego dane osobowe

zobowiązana jest natychmiast powiadomić Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego. W szczególności naruszenie bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym obejmuje wprowadzenie do systemu wirusów lub innych wrogich kodów, jak również dostęp do systemu informatycznego osób niepowołanych (fizyczny - poprzez bezpośredni dostęp do komputera, na którym przetwarzane są dane osobowe oraz logiczny - poprzez dostęp do danych osobowych za pośrednictwem sieci informatycznych). Szczegółowe zasady reagowania na incydenty związane z naruszeniem bezpieczeństwa danych osobowych są opisane w obowiązujących w Urzędzie Gminy Wilkowice procedurach postępowania, za których przygotowanie i uaktualnianie odpowiedzialny jest Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych.

Administrator Systemów Informatycznych jest odpowiedzialny za prowadzenie działań mających na celu zabezpieczenie systemu informatycznego przetwarzającego dane, w tym dane osobowe, przed zainfekowaniem wirusami lub innymi niebezpiecznymi kodami, a także za działania zmierzające do wykrycia ewentualnej infekcji i usunięcie jej skutków. Z tego względu Administrator Systemu Informatycznego ma prawo ograniczać uprawnienia użytkowników, w szczególności w zakresie wymiany informacji z wykorzystaniem publicznych sieci informatycznych, jeżeli może to wpłynąć na redukcję ryzyka wprowadzenia wirusów lub innych wrogich kodów do systemu informatycznego przetwarzającego dane osobowe i nie będzie miało wpływu na możliwość realizacji przez pracowników Urzędu Gminy Wilkowice ich obowiązków służbowych.

Pracownicy Urzędu Gminy Wilkowice korzystający z systemu informatycznego są zobowiązani do stosowania się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do przedmiotowych zaleceń wydawanych przez Administratora Systemu Informatycznego.

System informatyczny przetwarzający dane, w tym osobowe, powinien być wyposażony w techniczne i organizacyjne mechanizmy zabezpieczające możliwość realizacji krytycznych, z punktu widzenia ciągłości działania Urzędu Gminy Wilkowice oraz procesów związanych z przetwarzaniem tych danych.

Wszyscy pracownicy Urzędu Gminy Wilkowice mający dostęp do systemu informatycznego przetwarzającego dane osobowe są poddawani przeszkoleniu obejmującemu zapoznanie z obowiązującymi regulacjami prawnymi w zakresie ochrony tych danych, jak również obowiązującymi w Urzędzie Gminy Wilkowice zasadami bezpiecznego ich przetwarzania. Za organizację szkolenia odpowiada Administrator Bezpieczeństwa Informacji. Przeszkolenie pracownika jest warunkiem koniecznym do dopuszczenia go do korzystania z systemu informatycznego przetwarzającego dane osobowe.

Nieprzestrzeganie zasad ochrony danych osobowych zagrożone jest konsekwencjami karnymi, zgodnie z zapisami rozdziału 8 Ustawy.

Niniejsza polityka została zatwierdzona przez ..... UG..... w ..... w dniu: .....r.

WÓJT

Mieczysław Kączka

I.3 Znaczenie bezpieczeństwa informacji dla Urzędu

Sprawne realizowanie misji i celów Urzędu Gminy Wilkowice w wielu obszarach jest silnie uzależnione od niezakłóconej pracy jego systemów informacyjnych i bezpieczeństwa przetwarzanych w nich informacji.

Bezpieczeństwo informacji i teleinformatyczne jest tak silne jak jego najsłabsze ogniwo. W ciągłym doskonaleniu zawartych w dokumentacji zasad i praktyk dążymy do osiągnięcia jak najwyższego poziomu zabezpieczeń oraz eliminowaniu skutków działania ewentualnych zaistniałych incydentów. Jednym z najważniejszych aspektów ciągłego doskonalenia Urzędu Gminy Wilkowice jest koncentracja na ludziach i ich kompetencjach opartych na wiedzy, świadomości o istniejących zagrożeniach w zmieniających się realiach pracy urzędu.

I.4 Definicja bezpieczeństwa informacji

Utrzymanie bezpieczeństwa przetwarzanych przez Urząd Gminy Wilkowice informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie.

Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:

a. **Poufność informacji** - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,

b. **Integralność informacji** - rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,

c. **Dostępność informacji** - rozumiana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

d. **Zarządzanie ryzykiem** – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:

e. **Niezaprzeczalności odbioru** - rozumianej jako zdolność systemu Urzędu Gminy do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,

f. **Niezaprzeczalności nadania** - rozumianej jako zdolność systemu Urzędu Gminy do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie.

g. **Rozliczalności działań** – rozumianej jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania wykonał.

Ilekroć w dokumencie jest mowa o:

Administratorze Bezpieczeństwa Informacji (ABI) - rozumie się przez osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Bezpieczeństwa Informacji w odniesieniu do systemu nadzoru nad informacją (aktywami) w odniesieniu do systemów informatycznych;

Administratorze Systemów Informatycznych (ASI) - rozumie się przez osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Systemów Informatycznych w odniesieniu do systemu nadzoru nad informacją (aktywami) funkcjonującą w systemach informatycznych;

Administrator Danych Osobowych (ADO) - rozumie się przez to osobę pełniącą funkcje i posiadającą zakres uprawnień w rozumieniu ustawy o ochronie danych osobowych oraz pełniącą nadzór nad realizacją obowiązków wynikających z Polityki Bezpieczeństwa w urzędzie;

danych – rozumie się przez to dane będące w posiadaniu urzędu w postaci elektronicznej lub w innej formie, będące w zbiorach urzędu, wykorzystywane przez urząd lub osoby trzecie a niezbędne do wykonywania zadań urzędu;

danych osobowych – rozumie się przez to informacje o osobie fizycznej (a więc nie o osobie prawnej, chyba że jest to jednoosobowa spółka z ograniczoną odpowiedzialnością), dotyczące tożsamości tej osoby (w tym personalia umożliwiające jej identyfikację);

danych wrażliwych - rozumie się przez to dane określone w artykule 27 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późniejszymi zmianami), a więc dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

haśle - rozumie się przez to co najmniej 8-znakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie uprawnionej do pracy w systemie informatycznym, Administratorowi Danych Osobowych oraz Administratorowi Bezpieczeństwa Informacji;

identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez administratora danych osobowych obszarach systemu informatycznego urzędu;

incydent bezpieczeństwa – czynności, zjawiska naruszające zapisy Polityki Bezpieczeństwa Informacji oraz jej procedury mogące zagrozić utracie aktywów urzędu, ich integralności lub dostępności, a także dopuścić do nieuprawnionego dostępu do danych, jednoznaczne z sytuacją kryzysową;

procedurach ochrony danych osobowych – rozumie się przez to sposób przetwarzania danych osobowych oraz warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych w taki sposób, by zachować ich tajemnicę, zapewnić ochronę przed zniszczeniem i kradzieżą, określone wymogami ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późniejszymi zmianami), wymogami niniejszej Instrukcji;

przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, wprowadzanie do systemu urzędu, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie;

serwerze - rozumie się przez to jednostkę centralną, komputer zarządzający systemem informatycznym urzędu;

serwisancie - rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;

urząd - identyfikuje się jako samorządową jednostkę budżetową;

służbach informatycznych urzędu - rozumie się przez to informatyków zatrudnionych w urzędzie;

systemie informatycznym urzędu - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. W systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną urzędu;

systemy przetwarzania informacji tzn. informacje mogą być przetwarzane wyłącznie w systemach, które spełniają warunki opisane w PBI;

sytuacją kryzysową - jest to wystąpienie, zagrożenie lub domniemanie kradzieży, nieautoryzowanego dostępu, modyfikacji, zatajenia lub utraty (zniszczenia) przetwarzanej w systemie informacji zastrzeżonej. Każdy s ystem informatyczny (SI) powinien przechodzić okresowe audyty bezpieczeństwa;

użytkowniku - rozumie się przez to pracownika urzędu, zatrudnionego na podstawie umowy o pracę, umowy zlecenia lub innej umowy przewidzianej przepisami prawa oraz osobę odbywającą w urzędzie staż absolwencki, praktykę studencką, wolontariat, który przetwarza dane osobowe znajdujące się w zbiorach danych urzędu;

zbiorze danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych osobowych, dostępnych wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

I.5 Cele i strategie bezpieczeństwa Urzędu

Cele Urzędu Gminy Wilkowice w dziedzinie bezpieczeństwa informacji:

a. ochrona zasobów informacyjnych UG i zapewnienie ciągłości działania procesów Urzędu,
b. ochrona wizerunku Urzędu,
c. zapewnienie zgodności z prawem podejmowanych działań,
d. uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów UG rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,
e. wyznaczenie ogólnych kierunków rozwoju systemu informacyjnego,
f. podnoszenie kultury informatycznej i tworzenie bezpiecznego społeczeństwa informacyjnego.

Cele osiągane są przez realizowane strategie:

a. zapewnienie wsparcia Zarządzających dla Systemu Bezpieczeństwa Informacji,
b. właściwa organizacja Systemu Zarządzania Bezpieczeństwem Informacji,
c. zarządzanie ryzykiem w celu ograniczania go do akceptowanego poziomu,
d. właściwa ochrona informacji, a w szczególności informacji prawnie chronionych,
e. zapewnienie odpowiedniego poziomu dostępności informacji i niezawodności systemów informatycznych,
f. właściwa ochrona informacji związanych z zawartymi umowami,
g. wdrażanie i rozwój systemów informacyjnych z zachowaniem zasad bezpieczeństwa,
h. eksploatowanie systemów informacyjnych zgodnie z zasadami bezpieczeństwa,
i. stała edukacja użytkowników systemu informacyjnego.

I.6 Opis zdarzeń naruszających ochronę danych

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
   - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
   - nieuprawniony dostęp do systemu z jego wnętrza,
   - nieuprawniony przekaz danych,
   - pogorszenie jakości sprzętu i oprogramowania,
   - bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub kopiowano dane osobowe,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych

osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

I.7 Informacje przetwarzane przez system informacyjny Urzędu

W systemie informacyjnym Urzędu przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej i rozwoju instytucjonalnego.

Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

Przetwarzane w Urzędzie informacje są miedzy innymi informacjami dotyczącymi

a. informacji publicznych,
b. danych osobowych,
c. informacji stanowiących tajemnice Urzędu,
d. i innych informacji prawnie chronionych.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

W celu skutecznego zarządzania bezpieczeństwem przetwarzanych informacji zasoby informacyjne są podzielone na grupy informacji.

a. dla każdej grupy zidentyfikowane są zasoby uczestniczące w przetwarzaniu danej informacji,
b. dla każdej grupy zidentyfikowane są wymagania bezpieczeństwa, oszacowane jest ryzyko i na tej podstawie dobrane są odpowiednie zabezpieczenia.

I.8 Infrastruktura systemu informacyjnego Urzędu

Przetwarzanie informacji, w tym informacji osobowych odbywa, się we wszystkich lokalizacjach Urzędu to jest:

- w Wilkowicach przy ulicy Wyzwolenia 25

Część informacji przetwarzana jest również na komputerach przenośnych.

Rozmieszczenie stanowisk przetwarzających dane jest opisane w rozdziale I, punkcie 16.

I.9 Polityka Bezpieczeństwa Informacji jako System Zarządzania Bezpieczeństwem Informacji Urzędu

Polityka Bezpieczeństwa Informacji (PBI) traktowana jest jako podstawa Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Gminy Wilkowice opiera się na podejściu procesowym stosowanym w wymiarze instytucjonalnym.

W ramach systemu PBI wyróżniono proces zwany „Zarządzanie Ryzykiem".

Proces ten składa się z 4 integralnych działań:

- działanie przygotowania i wdrożenia Zarządzania Bezpieczeństwem Informacji:
    a. określenie zakresu systemu bezpieczeństwa informacji,
    b. analiza ryzyka,
    c. ocena ryzyka,
    d. przygotowanie procedur, standardów, regulaminów i innych dokumentów PBI,
    e. przygotowanie wdrożenia,
    f. wdrożenie PBI.

- działanie funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji:
    a. monitorowanie bezpieczeństwa informacji,
    b. planowanie i przeprowadzanie przeglądów i audytów bezpieczeństwa informacji,
    c. rejestracja incydentów,
    d. zarządzanie ryzykiem,
    e. działania korygujące i zapobiegawcze,
    f. doskonalenie PBI Urzędu Gminy Wilkowice,
    g. nadzór nad dokumentacją i zapisami.
- działanie zarządzania ciągłością działania:
    a. analiza zagrożeń,
    b. opracowanie planu ciągłości działania,
    c. testowanie planu ciągłości działania,
    d. doskonalenie planu ciągłości działania Urzędu Gminy Wilkowice,
    e. zastosowanie planu ciągłości działania,
    f. przywracanie stanu wyjściowego.
- działanie doskonalenia Polityki Zarządzania Bezpieczeństwa Informacji Urzędu Gminy Wilkowice:
    a. przegląd procesu zarządzania bezpieczeństwem,
    b. audyt bezpieczeństwa systemu,
    c. szkolenie kadry i propagowanie wiedzy o bezpieczeństwie informacji,
    d. doskonalenie polityk, procedur, standardów, regulaminów i innych dokumentów PBI Urzędu Gminy Wilkowice.

Sposób funkcjonowania Polityki Zarządzania Bezpieczeństwem Informacji regulują odrębne dokumenty wchodzące w skład Polityki Bezpieczeństwa Systemu teleinformacyjnego.

I.10 Struktura dokumentów Polityki Bezpieczeństwa Systemu Informacyjnego

Celem Polityki Bezpieczeństwa Informacji jest określenie zasad funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji.

Dokumenty ustanawiają metody zarządzania oraz wymagania niezbędne dla zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

Dokumenty Polityki Bezpieczeństwa Systemu Informacyjnego podzielone zostały na dwa poziomy:

a. dokumenty opisujące ogólne zasady bezpieczeństwa i zasady bezpieczeństwa dla poszczególnych grup informacji,
b. dokumenty opisujące zasady bezpieczeństwa systemów przetwarzania.

Zestaw dokumentów Polityki Bezpieczeństwa Systemu Informacyjnego składa się z następujących rodzajów dokumentów:

1. niniejszego dokumentu Polityki Bezpieczeństwa Systemu Informacyjnego opisującego:
   a. cele działań dotyczących zapewnienia bezpieczeństwa informacji,
   b. przyjęte strategie osiągnięcia celów ochrony informacji,
   c. opis struktury Polityki Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Systemu Informacyjnego,
   d. opis struktury odpowiedzialności za bezpieczeństwo informacji,
   e. podstawy prawne i normatywne Polityki Bezpieczeństwa Systemu Informacyjnego,
   f. zakres stosowania Polityki Bezpieczeństwa Systemu Informacyjnego,
   g. zakres rozpowszechniania niniejszego dokumentu.
2. dokumentu Zasad Zarządzania Bezpieczeństwem Informacji opisującego zasady zarządzania bezpieczeństwem informacji,
3. regulaminów opisujących szczegółowe zasady postępowania użytkowników systemu informacyjnego Urzędu,
4. instrukcji opisujących zasady wykonywania poszczególnych zadań,
5. dokumentów polityk bezpieczeństwa grup informacji określających szczegółowe wymagania bezpieczeństwa dla tych grup informacji,
6. dokumentów polityk bezpieczeństwa systemów przetwarzania informacji opisujących szczegółowe wymagania bezpieczeństwa poszczególnych systemów przetwarzania,
7. dokumentów procedur opisujących szczegółowe kroki działań podejmowanych w systemach przetwarzania,
8. dokumentów standardów opisujących konfigurację poszczególnych typów systemów przetwarzania.

Poszczególne dokumenty wymienione powyżej, będą tworzone sukcesywnie i wprowadzane w życie na podstawie poleceń służbowych Wójta Urzędu Gminy Wilkowice po zatwierdzeniu przez Administratora Bezpieczeństwa Informacji.

Dokumenty, o których mowa 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. z 2004r. Nr 100 poz. 1024) zostaną wprowadzone bądź w formie załączników do niniejszej Polityki bądź w formie odrębnych dokumentów wydanych na podstawie stosownych upoważnień.

I.11 Odpowiedzialność za bezpieczeństwo informacji

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Urzędu.

Nad przestrzeganiem postanowień Polityki Bezpieczeństwa Informacji i rozwojem Systemu Zarządzania Bezpieczeństwem czuwa Wójt Gminy Wilkowice.

W ramach Polityki Bezpieczeństwa Informacji traktowanej jako System Zarządzania Bezpieczeństwem wyróżnione zostały role na poziomie Polityki Bezpieczeństwa Informacji:

a. Administrator Bezpieczeństwa Danych Osobowych (ADO).....wójt
b. Administrator Bezpieczeństwa Informacji (ABI).....sekretarz
c. Administrator Bezpieczeństwa Systemu (ABS).....z-ca wójta
d. Administrator Systemu (AS).....gł.informatyk

Administrator Bezpieczeństwa Danych w tym Osobowych (ADO) jest odpowiedzialny za:

- realizację ustawy o ochronie danych, w tym danych osobowych w zakresie dotyczącym Administratora Danych,
- określanie jakiego rodzaju informacje mogą być przetwarzane w Urzędzie,
- określenie grup informacji przetwarzanych w Urzędzie,
- określanie czy Urząd jest właścicielem danej grupy informacji, czy też należy ona do innego podmiotu,
- ustalanie wykazu informacji stanowiących tajemnicę Urzędu.

Administrator Bezpieczeństwa Informacji (ABI) odpowiedzialny jest za:

- realizację ustawy o ochronie danych, w tym danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,
- zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione oraz że mogą one wykonywać wyłącznie uprawnione operacje,
- zabezpieczenie obszarów przetwarzania danych, w tym danych osobowych w sposób uniemożliwiający dostęp do nich osób trzecich,
- zgłoszenie konieczności uzupełnienia zakresu czynności osoby zatrudnionej przy przetwarzaniu danych o zakres odpowiedzialności tej osoby za ochronę danych do Administratora Informacji,
- ewidencjonowanie udostępniania danych zgodnie z ustawą o ochronie danych osobowych,
- weryfikację dopuszczenia użytkowników do przetwarzania danych,
- zatwierdzanie decyzji Administratora Informacji o przyznaniu danemu użytkownikowi identyfikatora w danym systemie przetwarzania,
- zatwierdzanie decyzji Administratora Informacji o przyznaniu danemu użytkownikowi praw dostępu do informacji chronionych w danym systemie przetwarzania,
- powiadomienie Administratora Systemu o konieczności utworzenia identyfikatora użytkownika w systemie,
- powiadomienie Administratora Systemu o zmianie uprawnień dostępu Użytkownika do systemu,

- prowadzenie rejestru osób dopuszczonych do przetwarzania grupy informacji chronionych,
- przygotowanie dokumentów polityki bezpieczeństwa danej grupy informacji chronionych,
- szkolenia osób dopuszczonych do danej grupy informacji chronionych, w tym zaznajomienie i przeszkolenie pracowników zatrudnionych przy przetwarzaniu danych osobowych z przepisami ustawy o ochronie danych osobowych i przepisami zawartymi w niniejszym zarządzeniu oraz za zebranie od nich oświadczeń o odbyciu takiego szkolenia,
- nadzorowanie podpisania stosownych umów o poufności pomiędzy użytkownikiem dopuszczonym do przetwarzania danej grupy informacji.

Administrator Bezpieczeństwa Systemu (ABS) jest odpowiedzialny za:

- poprawność merytoryczną danych gromadzonych w Zbiorach Danych za pomocą Aplikacji,
- określanie miejsca i czasu przetwarzania, przechowywania, tworzenia i niszczenia informacji należącej do danej grupy,
- określenie budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane,
- ewidencjonowanie lokalnych zbiorów danych osobowych wykorzystywanych w Urzędzie,
- określenie rodzaju Aplikacji oraz Urządzeń Komputerowych, które są niezbędne do realizacji zadań w Urzędzie Gminy Wilkowice,
- określenie wrażliwości grupy informacji ze względu na jej poufność, integralność i dostępność,
- określanie, które osoby i na jakich prawach mają dostęp do danych informacji,
- powiadomienie Administratora Bezpieczeństwa Informacji i Administratora Bezpieczeństwa Systemu o zakładaniu zbiorów danych na lokalnych urządzeniach komputerowych oraz w formie manualnej,
- określenie czasu rozpoczęcia i zakończenia pracy Użytkowników,
- zapewnienie Użytkownikowi stanowiska pracy zgodnie z powierzonymi obowiązkami,
- przygotowanie zgłoszenia rejestracji Zbiorów Danych do Generalnego Inspektoratu Danych Osobowych, jeżeli mają one charakter danych osobowych i przekazanie do Administratora Bezpieczeństwa Informacji,
- koordynację działań zapewniających sprawne funkcjonowanie i zabezpieczenie Systemu Informatycznego Urzędu przed niepowołanym dostępem,
- analizę raportów wszelkich zdarzeń związanych z bezpieczeństwem systemów przetwarzania informacji chronionych, otrzymywanych od Administratorów Systemów,
- dopuszczanie systemów przetwarzania informacji do eksploatacji,
- identyfikowanie systemów przetwarzania grup informacji chronionych w Urzędzie,
- zgodność wszystkich wdrażanych systemów przetwarzania informacji chronionych z Polityką Bezpieczeństwa Systemu Informacyjnego przyjętą w Urzędzie,
- zatwierdzanie dokumentów polityk bezpieczeństwa systemów przetwarzania informacji chronionych,

- zatwierdzanie procedur bezpieczeństwa i standardów zabezpieczeń zawnioskowanych i obowiązujących w Urzędzie Gminy Wilkowice przez AS,
- dokonywanie modyfikacji i akceptacji proponowanych zmian, jak i okresowych kontroli polityk i procedur,
- weryfikację i zatwierdzenie projektów rozwoju Systemu Informatycznego,
- nadzór nad wdrożeniem nowych aplikacji,
- umożliwienie przeprowadzenia kontroli Systemu Informatycznego Urzędu Gminy Wilkowice przez służby Biura Generalnego Inspektora Danych Osobowych,
- zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione i że mogą one wykonywać wyłącznie uprawnione operacje,
- kontrolę procesu przyznawania praw dostępu,
- przygotowanie dokumentów polityki bezpieczeństwa danego systemu przetwarzania informacji chronionych,
- przygotowanie dokumentów procedur zarządzania kontami użytkowników,
- przygotowanie dokumentów procedur kryzysowych związane z incydentami,
- określanie standardów dotyczących Urządzeń Komputerowych, Sieci Komputerowej, Oprogramowania Systemowego oraz Aplikacji pracujących w Systemie Informatycznym Urzędu w oparciu o informacje Administratora Systemu,
- przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

Administratora Systemu (AS) jest odpowiedzialny za:

- bieżący monitoring oraz zapewnianie ciągłości działania systemu informatycznego,
- optymalizację wydajności systemu informatycznego,
- instalację i konfigurację sprzętu sieciowego i serwerowego,
- instalację i konfigurację oprogramowania systemowego i sieciowego,
- konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
- konfigurację i administrację systemem pocztowym Urzędu,
- prowadzenie rejestru osób dopuszczonych do systemu (rejestr powinien zawierać: imię i nazwisko osoby, pełnioną rolę, grupę informacji, czas trwania dostępu),
- współpracę z dostawcami usług sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
- weryfikację możliwości integracji systemów informatycznych,
- zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego,
- zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
- opracowanie procedur określających zarządzanie systemem informatycznym,
- przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
- przyznawanie na wniosek Administratora Informacji, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie,

- udostępnianie danych zgromadzonych w Systemie Informatycznym, na wniosek Administratora Danych (w rozumieniu ustawy o ochronie danych osobowych) za zgodą Administratora Bezpieczeństwa Informacji,
- prowadzenie zakupów urządzeń sieciowych i serwerowych,
- prowadzenie zakupów oprogramowania sieciowego i serwerowego,
- wnioskowanie do Administratora Bezpieczeństwa Systemu Urzędu Gminy Wilkowice w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
- bieżący monitoring oraz zapewnianie ciągłość działania systemów baz danych,
- optymalizację wydajności systemów baz danych,
- instalację i konfigurację oprogramowania bazodanowego,
- konfigurację i administrację oprogramowaniem bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
- prowadzenie rejestru osób dopuszczonych do systemu baz danych (rejestr powinien zawierać: imię i nazwisko osoby, pełnioną rolę, grupę informacji, czas trwania dostępu),
- przyznawanie na wniosek Administratora Informacji, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych prawa dostępu do informacji w danym systemie bazodanowym,
- udostępnianie danych zgromadzonych w systemie bazodanowym, na wniosek Administratora Danych (w rozumieniu ustawy o ochronie danych osobowych) za zgodą Administratora Bezpieczeństwa Informacji,
- współpracę z dostawcami Aplikacji,
- nadzór nad wdrożonymi Aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, definiowanie słowników itp.),
- weryfikację możliwości integracji aplikacji bazodanowych,
- zapewnienie przeszkolenia Użytkowników w zakresie prawidłowego korzystania z aplikacji bazodanowych zgodnie z powierzonymi im obowiązkami,
- opracowanie procedur określających zarządzanie systemem bazodanowym,
- wykorzystywanie narzędzi baz danych dla tworzenia zestawień,
- definiowanie, obsługę i zarządzanie procesami pracy przy użyciu narzędzi WorkFlow,
- świadczeniu pomocy technicznej w ramach aplikacji bazodanowych dla użytkowników,
- przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

Praca Administratora Systemu i Sieci jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Systemu i Administratora Bezpieczeństwa Informacji.

I.12 Zakres stosowania Polityki Bezpieczeństwa Systemu Informacyjnego

Zasady określone przez dokumenty Polityki Bezpieczeństwa Systemu Informacyjnego mają zastosowanie do całego systemu informacyjnego Urzędu a w szczególności do:

- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
- informacji będących własnością Urzędu Gminy Wilkowice lub klienta UG, o ile zostały przekazane UG na podstawie umów,
- wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,
- wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
- wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa Systemu Informacyjnego zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, konsultanci, stażyści i inne osoby mające dostęp do informacji podlegającej ochronie.

I.13 Podstawy prawne

Polityka bezpieczeństwa odnosi się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w:

- ustawie z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101 poz. 926 z późniejszymi zmianami),
- ustawie z dnia 18.09.2001r. o podpisie elektronicznym (Dz.U. nr 130 poz.1450 z późniejszymi zmianami),
- ustawie o świadczeniu usług drogą elektroniczną z dnia 18.07.2002r. (Dz.U.nr 144 poz 1204 z późniejszymi zmianami),
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18.01.2001r. w sprawie Biuletynu Informacji Publicznej (Dz.U. Nr 10, poz.68),
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 roku, Nr 100, poz. 1024),
- rozporządzeniu Ministra Kultury z dnia 16.09.2002r. (Dz.U. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz.U. nr 167, poz.1375),
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 11.10.2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U. Nr 212, poz. 1766),
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 30.10.2006r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz.U. Nr 206 poz. 1517),
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 30.10.2006r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. Nr 206 poz. 1518),
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 27.11.2006r. w sprawie sporządzenia i doręczania pism w formie dokumentów elektronicznych (Dz.U.nr 227 poz. 1664).

I.14 Zakres rozpowszechniania

Z treścią niniejszego dokumentu powinni zapoznać się wszyscy pracownicy Urzędu i osoby mające dostęp do informacji przetwarzanej w Urzędzie.

Niniejszy dokument może być przedstawiany partnerom, z którymi Urząd związany jest odpowiednimi umowami.

I.15 Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane w tym dane osobowe

Zgodnie z rozporządzeniem wykonawczym do ustawy o ochronie danych osobowych z 29 kwietnia 2004r. (dz.U. z 2004r. nr 100 poz 1024 z póź. zmianami) ustanawia się wykaz pomieszczeń, w których wyłącznie możliwe jest przetwarzanie danych osobowych:

1) serwerownia zlokalizowana w budynku Urzędu Gminy zawierająca kluczowe części systemu przetwarzającego dane osobowe, w tym serwer baz danych i plików, system kopii zapasowych, elementy systemu zapewniające zasilanie awaryjne, stanowiska komputerowe dla administratorów.
2) pomieszczenie w którym znajdują się stanowiska komputerowe dla administratorów,
3) pomieszczenia działów: Finansowego, Kadr, Zamówień Publicznych, Oświaty, Obrony cywilnej, Gospodarki Komunalnej, Budownictwa, Urbanistyki, Rolnictwa, Ewidencji Działalności Gospodarczej, Ewidencji Ludności, Ochrony Środowiska, Gminnego Ośrodka Pomocy Społecznej, których pracownicy posiadają uprawnienia do przetwarzania danych oraz danych osobowych.

(Wszystkie wymienione wyżej pomieszczenia zlokalizowane są w Budynku Urzędu Gminy Wilkowice mieszczącym się przy ulicy Wyzwolenia 25)

Serwerownia musi być wyposażona w awaryjne źródło zasilania. Wejście do pomieszczenia jest wyposażone w drzwi o odpowiednich parametrach uniemożliwiające dostęp osobom niepowołanym. Podobnie wszystkie stanowiska, na których przetwarzane są dane osobowe wyposażone powinny być w urządzenia zapewniające zasilanie awaryjne.

I.16 Wykaz zbiorów danych, w tym danych osobowych wraz z obecnym miejscem przetwarzania

(w opracowaniu do wersji kolejnej)

Lp.	Nazwa zbioru danych	System/Program przetwarzający	Pokój nr
1.	Komputerowa baza ewidencji ludności gminy		
2.	Kartoteka płatników podatku od środków transportu gminy		
3.	Kartoteka kierowców gminy		
4.	Rejestr dzierżawy gruntów rolnych stanowiących własność agencji własności rolnej skarbu państwa w gminie		
5.	Rejestr decyzji o warunkach zabudowy i zagospodarowania terenu, informacje o działkach gminy		
6.	Elektroniczny rejestr ewidencji gruntów gminy		
7.	Rejestr wydanych dokumentów tożsamości gminy		
8.	Elektroniczna baza płatników podatku od nieruchomości od osób fizycznych, podatku rolnego i leśnego gminy		
9.	Rejestr kart osobowych aktualnych mieszkańców gminy		
10.	Rejestr kart osobowych byłych mieszkańców gminy		
11.	Rejestr osób zameldowanych na pobyt czasowy w gminie		
12.	Skorowidz alfabetyczny osób zameldowanych w gminie		
13.	Wykaz przedpoborowych gminy		
14.	Rejestr wydanych zezwoleń na wycięcie drzew na posesjach prywatnych gminy		
15.	Rejestr spraw dotyczących rozgraniczeń nieruchomości gruntowych gminy		
16.	Rejestr zaświadczeń o zaliczeniu do stażu pracy okresów pracy w indywidualnych gospodarstwach rolnych gminy		
17.	Lista poborowych gminy		
18.	Rejestr przedpoborowych gminy		
19.	Rejestr członków formacji obrony cywilnej gminy		
20.	Rejestr nadanych świadczeń rzeczowych i osobistych na rzecz obrony cywilnej gminy		
21.	Rejestr kurierów i posłańców gminy		
22.	Rejestr świadczeń osobistych i rzeczowych na rzecz uczestników akcji kurierskiej gminy		
23.	Zbiór danych dotyczących osób korzystających z pomocy Gminnego ośrodka Pomocy Społecznej gminy		
24.	Kartoteka spraw związanych z wydawaniem aktów własności dla gospodarstw rolnych gminy		
25.	Kartoteka spraw z zakresu podziałów nieruchomości gruntowych oraz łączeń działek gminy		
26.	Rejestr ewidencji gruntów gminy		
27.	Ewidencja osób o nieregulowanym stosunku do służby wojskowej gminy		
28.	Rejestr osób pobierających renty socjalne w Gminnym Ośrodku Pomocy Społecznej gminy		
29.	Rejestr osób pobierających zasiłki stałe w GOPS gminy		

30.	Rejestr osób pobierających zasiłki stałe wyrównawcze w GOPS w gminie		
31.	Rejestr osób pobierających zasiłki okresowe gwarantowane w GOPS gminy		
32.	Rejestr osób pobierających zasiłki okresowe w GOPS gminy		
33.	Rejestr osób pobierających zasiłki celowe w GOPS gminy		
34.	Rejestr osób pobierających zasiłki rodzinne i pielęgnacyjne w GOPS gminy		
35.	Wykaz najemców lokali usługowych gminy		
36.	Wykaz mieszkańców budynków komunalnych gminy		
37.	Zbiór teczek osobowych osób, którym wydano dokumenty tożsamości w gminie		
38.	Ewidencja zgłoszeń noworodków w gminie		
39.	Rejestr osób składających wnioski o wydanie dokumentu tożsamości w gminie		
40.	Ewidencja zdarzeń meldunkowych gminy		
41.	Ewidencja zdarzeń wynikających akt stanu cywilnego gminy		
42.	Rejestr numerów porządkowych budynków i nieruchomości i nazewnictwa ulic gminy		
43.	Rejestr kombatantów oraz osób będących ofiarami represji wojennych i okresu powojennego GOPS gminy		
44.	Kartoteka odbiorców wody i płatników za odprowadzanie ścieków gminy		
45.	Kartoteka czynszowa dla lokali usługowych gminy		
46.	Rejestr wydanych zezwoleń na sprzedaż wyrobów alkoholowych w gminie		
47.	Księgi Urzędu Stanu Cywilnego Gminy		
48.	Akta zbiorcze ksiąg USC gminy		
49.	Kartoteka czynszowa mieszkańców budynków komunalnych gminy		
50.	Dziennik płatników podatku od posiadania psa gminy		
51.	Kartoteka głównych lokatorów mieszkań służbowych nauczycieli, zatrudnionych w placówkach oświatowych gminy		
52.	Rejestr skarg i wniosków Urzędu Gminy		
53.	Rejestr wniosków o zmianę planu zagospodarowania przestrzennego gminy		
54.	Rejestr wydanych zezwoleń na budowę gminy		
55.	Kartoteka pojazdów gminy		