Zarządzenie Nr 11/2015
Wójta Gminy Sierakowice
z dnia 8 stycznia 2015 roku

w sprawie: dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Sierakowice

Na podstawie art. 36 ust.2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r. Nr 101, poz.926 z późn.zm). §3 i §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz.1024 z późn.zm)

Zarządzam, co następuje

§1

Wprowadza się do użytku służbowego:

1. Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Sierakowice stanowiąca załącznik Nr 1 do niniejszego zarządzenia
2. Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Sierakowice stanowiącą załącznik nr 2 do niniejszego zarządzenia

§2

Ilekroć w zarządzeniu jest mowa o:

1) *ustawie* – rozumie się przez to ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
2) *rozporządzeniu* – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
3) *zbiorze danych osobowych* – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie,
4) *przetwarzaniu danych* – rozumie się przez to jakiekolwiek operacje wykonywanych na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
5) *systemach informatycznych* – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedury, przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6) *zabezpieczeniu danych w systemie informatycznym* – rozumie się przez to wdrażanie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
7) *usuwaniu danych* – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
8) *urzędzie* – rozumie się przez to Urząd Gminy Sierakowice,
9) *administratorze systemu informatycznego* – rozumie się przez to osobę wyznaczona przez administratora danych odpowiedzialnego za funkcjonowanie systemu informatycznego
10) *użytkowniku* – rozumie się przez to użytkownika systemu, pracownika Urzędu Gminy upoważnionego przez administratora danych do przetwarzania danych osobowych,

11) *identyfikatorze użytkownika*- rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przeważania danych osobowych w systemie informatycznym,
12) *haśle* – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
13) *sieci telekomunikacyjnej* – rozumie się przez to sieć telekomunikacyjna w rozumieniu art.2 pkt 23 ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz.U. nr 73, poz.852 z późn.zm)
14) *sieci publicznej* – rozumie się przez to sieć publiczną w rozumieniu art.2 pkt 22 ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz.U. nr 73, poz.852 z późn.zm.)
15) *teletransmisji* – rozumie się przez to przesłanie informacji za pośrednictwem sieci telekomunikacyjnej
16) *rozliczności* – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi ,
17) *integralności danych* – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany
18) *raporcie* – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych osobowych,
19) *poufności danych* – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
20) *uwierzytelnianiu* – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§3

Zobowiązuje się Sekretarza Gminy do zapoznania z treścią zarządzenia wszystkich pracowników Urzędu.

§4

W sprawach nie uregulowanych niniejszym zarządzeniem zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

§5

Traci moc Zarządzenie Wójta Gminy Sierakowice Nr 25/2011 z dnia 02 maja 2011 roku w sprawie: dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Sierakowice oraz Zarządzenie Wójta Gminy Sierakowice Nr 106/2012 z dnia 31 grudnia 2012 roku *w sprawie: dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Sierakowice*

§6

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Tadeusz Kobiela

Załącznik nr 1
do zarządzenia
Nr.....

Polityka bezpieczeństwa

przetwarzania danych osobowych
w Urzędzie Gminy Sierakowice

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Sierakowice zwana dalej „Polityką bezpieczeństwa" określa i zawiera:

1) zasady ochrony dostępu do danych osobowych,
2) kontrola zabezpieczeń danych osobowych w systemie informatycznym,
3) tryb postepowania w sytuacji naruszenia ochrony danych osobowych,
4) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
5) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych,
6) opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informatycznych i powiązania między nimi,
7) sposób przepływu danych pomiędzy poszczególnymi systemami,
8) określenie sposobów technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczności przetwarzanych danych.

§1

Zasady ochrony dostępu do danych osobowych

1. Dane osobowe przetwarzane są w budynku Urzędu Gminy Sierakowice, ul. Lęborska 30 w pomieszczeniach lub częściach pomieszczeń tworząc obszar przetwarzania danych osobowych określony w załączniku Nr 1 do niniejszego dokumentu.
2. Przebywanie wewnątrz obszaru, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego osób nieupoważnionych jest możliwe tylko w obecności użytkownika i za zgodą administratora bezpieczeństwa informacji.
3. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na czas nieobecności użytkowników w sposób uniemożliwiający do nich dostęp osób nieuprawnionych.

4. Zabezpieczenie systemu informatycznego w zakresie nieuwzględnionym w „Polityce bezpieczeństwa" reguluje „Instrukcja zarządzania systemem informatycznym w Urzędzie Gminy Sierakowice" stanowiąca załącznik Nr 2 do niniejszego zarządzenia.

§2

Kontrola zabezpieczenia danych osobowych w systemie informatycznym

1. Codzienną kontrole zabezpieczenia danych w systemie informatycznym sprawuje użytkownik.
2. Administrator danych osobowych prowadzi bieżący nadzór nad przestrzeganiem przez użytkowników zasad ochrony danych osobowych oraz sprawuje kontrolę nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbiorów wprowadzone oraz komu są przekazywane.

§3

Tryb postepowania w sytuacji naruszenia ochrony danych osobowych

1. Za naruszenie ochrony danych osobowych uważa się w szczególności :

    1) próbę lub fakt nieuprawnionego dostępu do zbioru danych osobowych lub obszaru, w którym są one przetwarzane,
    2) sytuację, w której skutkiem jest:
        a) brak możliwości fizycznego dostępu do danych np. z powodu zgubienia klucza do pomieszczeń lub mebli biurowych, w których przechowywane są dokumenty zawierające przetwarzane dane osobowe, zniszczenia lub kradzieży urządzeń służących do przetwarzania danych osobowych w tym elektronicznych nośników informacji itp.
        b) brak dostępu do zbioru danych, np. zbiór istnieje lecz nie ma możliwości przetwarzania danych osobowych
        c) zmieniono zawartość zbioru, np. niepoprawna treść, postać, data, różnica w danych itp.
        d) różnica funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji
    3) zniszczenie lub próby zniszczenia w sposób nieautoryzowany danych ze zbiorów danych systemowych,
    4) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych,

5) nieskuteczne zniszczenie nośników informacji zawierających dane osobowe (nośniki elektroniczne, optyczne, warunki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione,
6) nieuprawnioną zmianę elementów systemu informatycznego służących do przetwarzania danych w szczególności urządzeń, procedur i oprogramowania.

2. W przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych użytkownik zobowiązany jest do:

1) określenia, w miarę możliwości charakteru zaistniałej sytuacji (np. kradzież, włamanie, wirus komputerowy, usunięcie bądź modyfikacja danych, uszkodzenia urządzenia itp.),
2) niezwłocznego zawiadomienia o zaistniałej sytuacji administratora bezpieczeństwa lub administratora danych oraz administratora systemu,
3) zabezpieczenia, w zależności od sytuacji dostępu do pomieszczenia i urządzenia służącego do przetwarzania danych osobowych, a także dowodów zdarzenia przed zniszczeniem,
4) powstrzymanie się od pracy w systemie informatycznym,
5) podjęcie działań stosownie do zaistniałej sytuacji, która zapobiegnie ewentualnej utracie danych osobowych,
6) sporządzeniu notatki służbowej z dokonanych ustaleń oraz podjęcie działań i przekazania jej osobom wymienionym w pkt 2.

3. W sytuacji, o której mowa w ust.2 administrator danych lub osoba przez niego upoważniona odpowiednio do swojej właściwości, zobowiązany jest do:

1) Oceny sytuacji uwzględniając stan pomieszczenia, w którym przetwarzane są dane osobowe, stan urządzenia oprogramowania i zbioru oraz identyfikacji zakresu ewentualnych negatywnych następstw ochrony danych osobowych,
2) Podjęcia działań mających na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszeń ochrony danych osobowych,
3) Podjęcia decyzji w sprawie ewentualnego odizolowania odpowiednich części systemu, dokonania przeglądu i kontroli zabezpieczeń wszystkich pozostałych elementów systemu,
4) Podjęcia działań mających na celu przywrócenie prawidłowego stanu zbiorom danych osobowych i elementów systemu informatycznego w tym zabezpieczenia,
5) Podjęcia decyzji co do dalszego postępowania, w tym dotyczącej przetwarzania danych osobowych w systemie informatycznym,

6) Sporządzenie notatki służbowej z dokonanych ustaleń oraz podjętych działań i przekazanie jej administratorowi bezpieczeństwa informacji, w przypadku jego nieobecności administratorowi danych. Notatka powinna zawierać informacje o przyczynach, skutkach, a także winnych naruszenia ochrony danych i czy naruszenie danych osobowych było wynikiem przestępstwa oraz wnioski określające zakres działań technicznych i organizacyjnych niezbędnych do podjęcia w celu zapobieżenia w przyszłości naruszeniu ochrony danych osobowych.

§4

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych stanowi załącznik Nr 2 do „Polityki bezpieczeństwa"

§5

Opis struktury zbiorów wskazujący zawartość poszczególnych pól informatycznych i powiązania między nimi stanowi załącznik Nr 3 do „Polityki bezpieczeństwa"

§6

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczności przetwarzanych danych

I) Środki ochrony fizycznej w budynku Urzędu Gminy w Sierakowicach przy ul. Lęborskiej 30

1. Dostęp do budynku, w którym zlokalizowany jest obszar przetwarzania danych osobowych nadzorowany jest przez pracowników ochrony poza godzinami pracy urzędu.
2. Budynek, w którym znajduje się obszar przetwarzania danych osobowych dodatkowo zabezpieczony jest elektronicznym systemem antywłamaniowym oraz wydzielonym systemem przeciwpożarowym. Oba systemy ściśle współpracują z systemem powiadamiania pracowników ochrony.
3. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi. Pracownicy zobowiązani są zamykać pomieszczenia na czas ich nieobecności.
4. Kopie zapasowe przechowywane są w pomieszczeniu zabezpieczonym zamkiem patentowym oraz odrębnym elektronicznym systemem antywłamaniowym.

II) Środki sprzętowe, informatyczne i telekomunikacyjne

1. Zastosowano niszczarki dokumentów
2. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej.
3. Dane są przetwarzane w sposób zdecentralizowany
4. Sieć lokalna podłączona jest do Internetu za pomocą sprzętowego urządzenia (modem ADSL z mechanizmem NAT.
5. Dostęp do sieci z zewnątrz możliwy jest tylko na podstawie odrębnej umowy. Dostęp taki jest zabezpieczony za pomocą szyfrowanego bezpiecznego połączenia VPN.
6. Kopie awaryjne wykonywane są na twardym dysku zabezpieczonym w odrębnym pomieszczeniu zabezpieczonym zamkiem patentowym oraz odrębnym elektronicznym systemem antywłamaniowym.

III) Środki ochrony w ramach oprogramowania urządzeń teletransmisji.

1. Zastosowano sprzętowy firewall umiejscowiony w serwerowni.
2. Wszystkie komputery chronione są programem antywirusowym działającym w tle. Uaktualnianie baz wirusowych następuje automatycznie każdego dnia bezpośrednio po uruchomianiu komputera.
3. Sprzętowy firewall chroniony jest hasłem dostępu.

IV) Środki ochrony w ramach oprogramowania systemu

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla Administratora Bezpieczeństwa Informacji.
2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji (w przypadku systemów bazodanowych)
3. Zastosowano oprogramowanie do tworzenia kopii zapasowych.
4. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
5. Na komputerach użytkowników zastosowano program antywirusowy.
6. W systemie operacyjnym zastosowano mechanizm wymuszający okresowa zmianę dostępu do sieci.
7. Każdorazowo odnotowuje się próby podłączenia sprzętu zewnętrznego do infrastruktury służbowej.

V) Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

1. Automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego dane oraz datę pierwszego wprowadzenia danych
2. Zainstalowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
3. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator

VI) Środki ochrony w ramach systemu użytkowego

1. Zastosowano wygaszacze ekranu w przypadku dłuższej nieaktywności użytkownika
2. Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.
3. W przypadku służbowych urządzeń mobilnych zastosowano szyfrowanie dysku.

VII) Środki organizacyjne

1. Wyznaczono Administratora Systemu Informatycznego
2. Tymczasowe wydruki z danymi osobowymi są niszczone po ustaniu ich przydatności.
3. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy
4. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych osobowych oraz informowanie o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemach informatycznych.
5. Następuje niezwłoczna zmiana uprawnień w przypadku zmiany zadań osób wymienionych w punkcie 4
6. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych
7. Ustalono instrukcję zarządzania systemami informatycznymi.
8. Zdefiniowano procedury postepowania w sytuacji :
    a) Naruszenia ochrony danych osobowych,
    b) Słabości systemu
    c) Niewłaściwego funkcjonowania oprogramowania

9. Rejestracji podlegają wszystkie przypadki awarii systemu, działania konserwacyjne w systemie oraz naprawy systemu.

10. W przypadku gdy zachodzi konieczność naprawy sprzętu poza siedzibą Urzędu, należy wymontować z niego nośniki zawierające dane osobowe.
11. W przypadku gdy uszkodzenie sprzętu zawierającego nośnik informacji, na którym zapisane są dane osobowe, np. dysk twardy, jest tego rodzaju, że konieczne jest przekazanie sprzętu poza siedzibę urzędu, nośniki te wymontowuje się , a następnie niszczy.
12. Zapewniony jest okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
13. Zapewnia się szkolenia ze znajomości przepisów o ochronie danych osobowych oraz kontrole znajomości tych przepisów.

Załącznik Nr 1 do
POLITYKI BEZPIECZEŃSTWA

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

Lokalizacja obiektu	Komórki organizacyjne	Nr pokoju	Rodzaj sprawy
Budynek Urzędu Gminy ul. Lęborska 30 Sierakowice	Referat Spraw Obywatelskich	120 121	Ewidencja Ludności Dowody Osobiste Księgi USC
	Radca Prawny	317	Prawnicze
	Pełnomocnik Wójta ds. osób Niepełnosprawnych	111	Sprawy osób niepełnosprawnych
	Pełnomocnik Wójta ds. Profilaktyki i Rozw. Probl. Alkoh.	302	Profilaktyka antyalkoholowa
	Audytor wewnętrzny	217	Sprawy audytowe
	Komórka ds. unijnych	202 201	- Programy pomocowe - Koordynacja z Unią Europejską
	Referat Podatkowy	205 208	Wymiar podatku
	Gospodarka Gruntami	301	Informacje gruntowe
	Ochrona Środowiska	302,111	Ochrona środowiska, Ewidencja opłat śmieciowych
	Referat Rolnictwa	108 109	Sprawy rolnicze
	Referat Gospodarki Komunalnej	312	Dodatki mieszkaniowe, najem
	Kancelaria Urzędu	102	
	Kadry Płace	202 228	Sprawy Kadrowo Płacowe
	Dział świadczeń rodzinnych	318 320 321	Dodatki rodzinne Fundusz Alimentacyjny
	Informatyk	217	Sprawy Informatyczne
	Skarbnik	218	Sprawy finansowe
	Księgowość Budżetowa	215	Sprawy finansowe
	Obsługa Rady Gminy	211	Sprawy zaświadczenia zeznania
	Budownictwo	303	Sprawy budowlane

Załącznik Nr 2 do
POLITYKI BEZPIECZEŃSTWA

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

1. Wykaz zbiorów danych osobowych prowadzonych w systemach informatycznych.

Wszystkie zbiory oraz terminale znajdują w budynku Urzędu Gminy Sierakowice

Lp	Rodzaj zbioru	Typ zbioru	Nazwa programu	Terminale	Fizyczne położenie zbioru
1	Ewidencja Ludności	INF	ELUD PLUS - RADIX	Pok. 120,301,303,318	Pokój 220
2	Ewidencja Płatników i Windykacja	INF	WIP - RADIX	Pok. 205,312	Pokój 220
3	Ewidencja pracowników urzędu	INF	KADRY+ RADIX	Pok.228, 202	Pokój 202
5	Ewidencja wynagrodzeń pracowników urzędu	INF	PŁACE+ RADIX	Pok. 228, 202	Pokój 202
6	Ubezpieczenia społeczne	INF	PŁATNIK - ASSECO	Pok. 202,321	Pok. 202,321
8	Rejestr podatku transportowego	INF	POST PLUS RADIX	Pok. 312	Pokój 220
9	Ewidencja podatników – podatek od nieruchomości	INF	POGRUN RADIX	Pok. 111,108,205, 208, 302	Pokój 220
10	Rejestr decyzji o zwrocie podatku akcyzowego	INF	EXCEL -autorski	Pokój 108	Pokój 108
11	Rejestr Aktów Stanu Cywilnego	INF	PB_USC Technika Gliwice	Pokój 121	Pokój 121
12	Rejestr decyzji o warunkach zabudowy	INF	EXCEL autorski	Pokój 303	Pokój 303
13	Rejestr umów na wywóz śmieci i ścieki	INF	OWG PROFECO	Pokój 111,302	Pokój 302
14	Ewidencja podmiotów gospodarczych	INF	EPOD RADIX	Pokój 208	Pokój 220
15	Ewidencja uczestników projektów współfinansowanych ze funduszy UE	INF	PEFS	Pokój 202,203	Pokój 202,203
16	Ewidencja osób korzystających ze świadczeń rodzinnych oraz funduszu alimentacyjnego		Fundusz Alimentacyjny ZETO KOSZALIN ,	Pokój 318-321	Pokój 318-321,220
17	Ewidencja dłużników alimentacyjnych		Świadczenia rodzinne ZETO KOSZALIN	Pokój 318-321	Pokój 318-321,220

2. Wykaz zbiorów danych osobowych prowadzonych metodą tradycyjną

Lp	Nazwa zbioru	Lokalizacja zbioru	Uwagi
1	Księgi stanu cywilnego	Pok. 122	
2	Dowody osobiste	Pok. 120	
3	Wykaz opłat za przekształcenie prawa użytkowania wieczystego w prawo własności	Pok. 301	
4	Rejestr opłat za użytkowanie wieczyste	Pok. 301	
5	Rejestr kwalifikacji poborowych	Pok. 121	
6	Rejestr wypadków przy pracy	Pok. 238	
7	Rejestr zawartych umów	Pok. 218,312,201,202	
8	Rejestr zaświadczeń	Pok. 312	
9	Oświadczenia majątkowe radnych i innych osób na które ustawa nakłada obowiązek ich składania	Pok.113	
10	Rejestr dodatków mieszkaniowych	Pok.312	
11	Ewidencja osób korzystających ze świadczeń rodzinnych oraz funduszu alimentacyjnego	Pokój 318-321	
12	Ewidencja dłużników alimentacyjnych	Pokój 318-321	

Załącznik Nr 3 do
POLITYKI BEZPIECZEŃSTWA

Opis struktury zbioru danych

Lp	Rodzaj zbioru	Struktura zbioru	Powiązania pomiędzy polami informacyjnymi
1	Ewidencja Ludności	Imię/Imiona i nazwisko, nr PESEL,NIP lub REGON, data urodzenia, imiona rodziców, adres zamieszkania, data zameldowania na pobyt stały/czasowy	
2	Ewidencja Płatników i Windykacja	Imię/Imiona i nazwisko, nr PESEL,NIP lub REGON, data urodzenia, imiona rodziców, adres zamieszkania.	
3	Ewidencja pracowników urzędu	Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania lub pobytu, data przyjęcia do pracy, stanowisko, wykształcenie, sposób nawiązania stosunku pracy, sposób rozwiązania stosunku pracy, data zwolnienia	
4	Ewidencja wynagrodzeń pracowników urzędu	Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania lub pobytu, data przyjęcia do pracy, stanowisko, zawód	
5	Ubezpieczenia społeczne	Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania lub pobytu, data przyjęcia do pracy, stanowisko, zawód	
6	Rejestr podatku transportowego	Imię/Imiona i nazwisko, nr PESEL,NIP lub REGON, data urodzenia, imiona rodziców, adres zamieszkania.	
7	Ewidencja podatników – podatek od nieruchomości	Imię/Imiona i nazwisko, nr PESEL,NIP lub REGON, data urodzenia, imiona rodziców, adres zamieszkania.	
8	Rejestr decyzji o zwrocie podatku akcyzowego	Imię/Imiona i nazwisko, nr PESEL,NIP, powierzchnia użytków rolnych, numer konta bankowego	

9	Rejestr Aktów Stanu Cywilnego	Imię/Imiona i nazwisko, nr PESEL,NIP lub REGON, data urodzenia, imiona rodziców, adres zamieszkania, stan cywilny	
10	Rejestr decyzji o warunkach zabudowy	Imię i nazwisko, adres zamieszkania, nr i położenie nieruchomości, rodzaj planowanej inwestycji	
11	Rejestr umów na wywóz śmieci i ścieki	Imię i nazwisko, adres zamieszkania, nr i położenie nieruchomości	
12	Ewidencja podmiotów gospodarczych	Imię/Imiona i nazwisko, nr PESEL, NIP, data urodzenia, adres zamieszkania.	
13	Ewidencja osób korzystających ze świadczeń rodzinnych oraz funduszu alimentacyjnego	imię, nazwisko, NIP, PESEL, data urodzenia, adres zamieszkania, seria i nr dowodu tożsamości/ karta stałego pobytu	
14	Ewidencja dłużników alimentacyjnych.	imię, nazwisko, NIP, PESEL, data urodzenia, adres zamieszkania, seria i nr dowodu tożsamości	
15	Ewidencja uczestników projektów współfinansowanych ze funduszy UE	Imię i nazwisko, nr PESEL, data i miejsce urodzenia, adres zamieszkania, nr telefonu, e-mail, status na rynku pracy, wykształcenie.	
16	Księgi stanu cywilnego	Imię i nazwisko, nr PESEL, data i miejsce urodzenia, adres zamieszkania	
17	Dowody osobiste	Imię i nazwisko, nr PESEL, data i miejsce urodzenia, adres zamieszkania	
18	Wykaz opłat za przekształcenie prawa użytkowania wieczystego w prawo własności	Imię i nazwisko, adres zamieszkania, powierzchnia nieruchomości objętej opłatą	
19	Rejestr opłat za użytkowanie wieczyste	Imię i nazwisko, adres zamieszkania, powierzchnia nieruchomości objętej opłatą	
20	Rejestr kwalifikacji poborowych	Imię, nazwisko, imię ojca, PESEL, adres zamieszkania, rok urodzenia, informacje o stanie zdrowia	
21	Rejestr zawartych umów (dzierżawy, lokali komunalnych)	Imię i nazwisko/Nazwa firmy, adres zamieszkania, PESEL, NIP, REGON, KRS, forma działalności	
22	Rejestr zaświadczeń	Imię i nazwisko, adres, wysokość dochodów z gospodarstwa rolnego, wielkość gospodarstwa, posiadanie nieruchomości	

23	Oświadczenia majątkowe radnych i innych osób na które ustawa nakłada obowiązek ich składania	Imię i nazwisko, data i miejsce urodzenia, adres zamieszkania, zasoby pieniężne, zobowiązania, nieruchomości, udziały, akcje, działalność gospodarcza, stanowisko zajmowane w spółkach	
24	Rejestr dodatków mieszkaniowych	Imię i nazwisko, adres, data urodzenia, stan cywilny, dochód osób w gospodarstwie domowym uprawnionym do dodatku	
25	Ewidencja płatników opłaty śmieciowej	Imię i nazwisko, adres zamieszkania, nr dowodu osobistego, PESEL, Numer telefonu, adres e-mail, ilość osób w gospodarstwie domowym,	

Załącznik Nr 4 do
POLITYKI BEZPIECZEŃSTWA

Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami

Lp.	Nazwa zbioru	Sposób przepływu danych pomiędzy poszczególnymi systemami
1.	ELUD PLUS EWIDENCJA LUDNOŚCI	ELUD PLUS-->POGRUN ELUD PLUS -->WIP ELUD PLUS -->OWG ELUD PLUS -->KADRY
2.	KADRY	KADRY-->PŁACE
3.	POST PLUS Podatki od środków transportu	POST PLUS-->WIP
4.	POGRUN Podatki lokalne	POGRUN--> WIP POGRUN-->OWG
6.	OWG System obsługi podatku śmieciowego	ELUD-->OWG POGRUN-->OWG
7.	WIP Windykacja i podatki	ELUD PLUS-->WIP
8.	PŁATNIK Obsługa ZUS	PŁACE-->PŁATNIK
9.	PŁACE	KADRY-->PŁACE-->PŁATNIK

Załącznik nr 2
do zarządzenia Nr 25/2011
Wójta Gminy Sierakowice
z dnia 02 maja 2011r.

Instrukcja
Zarządzania Systemem Informatycznym

służącym do przetwarzania danych osobowych
w Urzędzie Gminy w Sierakowicach

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Sierakowice określa i zawiera:

1) Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
2) Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,
3) Procedury rozpoczęcia, zawieszenia, zakończenia pracy w systemie informatycznym,
4) Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5) Sposób, miejsce oraz okres przechowywania:
    a) Elektronicznych nośników informacji zawierających dane osobowe
    b) Kopii zapasowych, o których mowa w pkt 4,
6) Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
7) Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
8) Sposób realizacji wymogu odnotowania przez system informacji o odbiorcach:

§1

Procedura nadawania uprawnień do przetwarzania danych i rejestrowania uprawnień w systemie informatycznym, wskazanie osoby odpowiedzialnej za te czynności.

A. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Nadawanie uprawnień i rejestrowanie użytkownika w systemie wymaga spełnienia następujących warunków:

a) podpisanie przez osobę, ubiegającą się o dostęp, stosownego oświadczenia wg wzoru stanowiącego załącznik Nr 4 do zarządzenie nr .... z dnia 02 maja 2011r. - dotyczącego zapoznania się z przepisami o ochronie danych osobowych i zobowiązania do zachowania w tajemnicy informacji związanych z ich przetwarzaniem,

b) wydanie przez Administratora Danych stosownego upoważnienia użytkownika do przetwarzania danych osobowych w systemie informatycznym,

c) zarejestrowanie w/w upoważnienia w ewidencji wydanych upoważnień,

d) dokonanie zmian w ewidencji osób zatrudnionych i upoważnionych do przetwarzania danych osobowych

2. Z chwilą zarejestrowania w systemie użytkownik jest informowany przez Administratora Bezpieczeństwa Informacji o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.

3. Użytkownika wyrejestrowuje się z systemu po utracie uprawnień dostępu do przetwarzania danych, co może mieć miejsce w sytuacjach:
    a) ustania zatrudnienia użytkownika u Administratora Danych,
    b) zmiany zakresu obowiązków użytkownika.

4. Rozwiązanie umowy o pracę powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu, wykreślenie identyfikatora z ewidencji oraz unieważnienie jego hasła.

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

1. Systemy informatyczne, w których przetwarza się dane osobowe w zbiorach urzędu muszą być wyposażone w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do nich. W urzędzie do uwierzytelniania użytkowników stosuje się hasła.

2. Procedury związane z zarządzaniem i użytkowaniem hasła:
    a) każdemu użytkownikowi zarejestrowanemu w systemie Administrator Bezpieczeństwa Informacji nadaje identyfikator,
    b) identyfikator użytkownika wpisuje się do ewidencji osób zatrudnionych i upoważnionych do przetwarzania danych osobowych oraz rejestruje w systemie.

3. Użytkownik systemu posiada indywidualny identyfikator I hasło oddzielnie dla sieci i aplikacji,

4. Każdy użytkownik sam ustala dla siebie hasła dostępu do systemu,

5. Hasło składa się z co najmniej 8 znaków, zawierających małe i wielkie litery

oraz cyfry lub znaki specjalne,

6. Hasło dostępu do sieci dla użytkownika zmienione jest nie rzadziej niż co 30 dni. System sieciowy wymusza zmianę hasła,
7. Hasła dostępu do aplikacji dla użytkownika zmieniane są co kwartał. Administrator Bezpieczeństwa Informacji kontroluje zmianę hasła
8. Hasła dostępu zapisywane są na ekranie monitora w formie niejawnej i mogą być znane tylko użytkownikowi,
9. Hasła użytkownika umożliwiające dostęp do systemu informatycznego należy utrzymać w tajemnicy również po upływie ważności,

C. Procedury rozpoczęcia, zawieszenia, zakończenia pracy w systemie informatycznym:

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego, a w szczególności:
    a) przed wejściem do pomieszczenia sprawdzić czy na drzwiach i zamkach nie ma widocznych siadów prób niepowołanego ich otwierania,
    b) sprawdzić stan okien oraz ocenić czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób trzecich,
    c) sprawdzić stan sprzętu informatycznego oraz zamknięcie szaf i biurek,
    d) po włączeniu komputera ocenić jakość jego pracy i stwierdzić ewentualne zmiany.
2. Użytkownik przed przystąpieniem do przetwarzania danych powinien załogować się w systemie, posługując się swoim identyfikatorem i hasłem.
3. Użytkownik w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:
    a) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwiać podgląd osób trzecich,
    b) stosować urządzenia zabezpieczające przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci elektrycznej. Potrzeby w tym zakresie zgłaszają Administratorowi Bezpieczeństwa Informacji - przełożeni użytkownika,
    c) w przerwach w pracy uniemożliwia się wgląd osobom trzecim poprzez wygaszanie ekranu.
    d) opuszczając stanowisko pracy należy opuścić aplikacje bazo-danową i zakończyć pracę w sieci celem zapobiegnięcia dostępu osób trzecich.
4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:
    a) wylogować się z systemu : zaczekać na jego wyłączenie się,
    b) sprawdzić czy nie zostały pozostawione bez. nadzoru nośniki informacji,
    c) upewnić się, że szafy i biurka z dokumentacją są zamknięte,

d) wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie i klucze odnieść do sekretariatu.

5. Po godzinach pracy zapewnia się dozór całego budynku, pomieszczenia wyposażone są w okna PCV lub antywłamaniowe oraz w czujkę alarmową.
6. W przypadku stwierdzenia przez użytkownika prób niepowołanego naruszenia zabezpieczenia fizycznego pomieszczenia, zmian w systemie bezpieczeństwa systemu lub zauważenia, że stan urządzeń, zawartość zbiorów danych, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie danych osobowych natychmiast należy poinformować Administratora Bezpieczeństwa Informacji i przełożonego.

D. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1. Kopie zapasowe tworzy i przechowuje Administrator Bezpieczeństwa Informacji.
2. Kopie zapasowe należy wykonywać na bieżąco, obowiązkowo na koniec każdego miesiąca.

E. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych:

1. Tworzy się trzy rodzaje tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania zgromadzonych na serwerze:
   a) Archiwizacja codzienna – przyrostowa.
      - Archiwizacja zawiera tylko i wyłącznie dane - pliki baz danych, które uległy zmianie od czasu wykonania poprzedniej archiwizacji,
      - wykonuje się po zakończeniu każdego dnia pracy,
      - wykonywana jest na dysku optycznym lub taśmie streamera,
      - ostatnia kopia przechowywana jest w miejscu specjalnie do tego przeznaczonym poza budynkiem urzędu,
      - pozostałe kopie przechowywane są w wydzielonej części szafy pancernej.

   b) Archiwizacja tygodniowa-całościowa
      - archiwizacja zawiera wszystkie dane - pliki baz danych przetwarzanych w urzędzie, dot. zbiorów gromadzonych na woluminach serwerów,
      - archiwizacja wykonywana jest na dysku optycznym (taśmie streamer'a)
      - ostatnia kopia przechowywana jest w miejscu specjalnie do tego przeznaczonym poza budynkiem urzędu,
      - pozostałe kopie przechowywane są w wydzielonej części szafy pancernej.

c) Archiwizacja miesięczna – systemowa

- archiwizacja zawiera zbiory baz danych i aplikacje je obsługujące oraz dokumenty użytkowników sieci,
- archiwizacja wykonywana jest na dysku optycznym (taśmie streamer'a). Jeden dysk optyczny jest przyporządkowany jednemu miesiącowi,
- kopię miesięczną wykonuje się niezależnie od kopii tygodniowej
- w styczniu każdego roku niszczone są kopie roku poprzedniego za wyjątkiem płyt z grudnia danego roku,
- kopia przechowywana jest w kasecie ogniotrwałej.

2. Kopie zapasowe zawierające dane osobowe zgromadzonych na lokalnych stanowiskach komputerowych:
   a) wykonuje samodzielnie użytkownik w porozumieniu z Administratorem Bezpieczeństwa Informacji,
   b) należy tworzyć na odpowiedniej jakości nośnikach informacji,
   c) należy przechowywać w innych pomieszczeniach niż zbiory danych osobowych, lub w miejscach wskazanych przez przełożonego, zapewniających im odpowiednie warunki bezpieczeństwa.
3. Użytkownik i Administrator Bezpieczeństwa Informacji systematycznie sprawdzają kopie zapasowe i określają ich przydatność do wykorzystania w wypadku awarii systemu.
4. Zdezaktualizowane i uszkodzone kopie zapasowe należy mechanicznie niszczyć w sposób uniemożliwiający ich ponowne użycie.

F. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:

1. Użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów komputerowych. Czynność ta jest zaprogramowana w systemie, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji.
2. Kontrola antywirusowa systemu obejmuje wszystkie nośniki informacji, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
3. Obowiązkiem Administratora Bezpieczeństwa Informacji jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego.
4. Po każdorazowym wykryciu wirusa użytkownik zobowiązany jest niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności.

G. Sposób realizacji wymogu odnotowania przez system informacji o odbiorcach:

Informacje o danych osobowych przetwarzanych w systemie informatycznym przekazywane są w urzędzie wyłącznie z systemów ELUD, PŁATNIK oraz POGRUN. Jedynymi odbiorcami danych osobowych są:
TBD w Gdańsku
CBD w Warszawie
ZUS w Gdańsku
GUS w Warszawie
Każda przekazywana informacja jest ewidencjonowana. Data i zakres udostępnionych danych odnotowywany jest automatycznie w systemie.

H. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1. Okresowe przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania urzędu wykonuje Administrator Bezpieczeństwa Informacji.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw w autoryzowanych firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych, naprawia się je pod nadzorem Administratora Bezpieczeństwa Informacji lub sporządza się umowę powierzenia przetwarzania danych osobowych.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku gdy nie jest to możliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.
4. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do przekazania innemu podmiotowi, który nie jest uprawniony do otrzymania takich danych, należy wcześniej pozbawić zapisów danych.
5. Czynności, o których mowa w ust. 3 i 4 wykonuje komisja powołana przez Administratora Danych, której przewodniczy Administrator Bezpieczeństwa Informacji.

Postanowienia końcowe

1. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje Administrator Bezpieczeństwa Informacji.
2. Zabrania się korzystania z ogólnodostępnych komunikatorów (tj. gadu-gadu, skype, tlen itp.) oraz programów p2p tzn. mule, torent itp. Blokuje się dostęp do stron typu: Faceebok, allegro, itp.

3. Dopuszcza się korzystanie tylko z firmowych kont poczty elektronicznej. Wykorzystywanie kont prywatnych do korespondencji służbowej jest zabronione.
4. Zabrania się kopiowania dokumentów zawierających dane osobowe na prywatne nośniki informacji /pen drivy, dyskietki, inne urządzenia mobilne/.
5. Użytkownik komputera przenośnego służbowego zawierającego dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza budynkiem urzędu, w tym stosuje się partycję typu NTFS uniemożliwiającą odczyt danych bez znajomości loginu i hasła. Nie dopuszcza się możliwości korzystania ze sprzętu prywatnego i podłączania go do infrastruktury służbowej.
6. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest zapoznać się z niniejszą instrukcją i stosować jej przepisy na swoim stanowisku pracy.
7. Nadużycie przez użytkownika postanowień niniejszej instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.