POLITYKA BEZPIECZEŃSTWA INFORMACJI

oraz

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

SPIS TREŚCI

Załącznik Nr 1
do Zarządzenia Nr 0152/30/2008
Wójta Gminy Psary z dnia 25.06.2008 r.
w sprawie: Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
Systemu Informatycznego Urzędu Gminy w Psarach

POLITYKA BEZPIECZENSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
SYSTEMU INFORMATYCZNEGO URZĘDU GMINY w PSARACH

Podstawa prawna:

- 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 (Dz. U. Nr 100, poz. 1024)
- ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z pózn. zm.)
- jeśli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę niż wynika to z ustawy o ochronie danych osobowych, stosuje się przepisy tych ustaw.

I. Definicje.

Ilekroć w niniejszym dokumencie jest mowa o:

a) **Urzędzie** – należy przez to rozumieć Urząd Gminy Psary,

b) **Kierowniku Urzędu** – należy przez to rozumieć Wójta Gminy Psary,

c) **Administratorze Danych** – należy przez to rozumieć Wójta Gminy Psary,

d) **Administratorze Bezpieczeństwa Informacji** – należy przez to rozumieć pracownika Urzędu Gminy w Psarach lub inną osobę wyznaczoną do nadzorowania oraz przestrzegania zasad ochrony danych osobowych – ustanowionych zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu Gminy w Psarach,

e) **Administratorze Systemu Informatycznego** – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego Urzędu Gminy w Psarach oraz stosowanie technicznych i organizacyjnych środków ochrony,

f) **użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy w Psarach. Użytkownikiem może być pracownik Urzędu Gminy w Psarach, osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno - prawnej, osoba odbywająca staż lub praktykę w Urzędzie Gminy w Psarach,

g) **sieci lokalnej** – należy przez to rozumieć połączenie systemów informatycznych Urzędu Gminy w Psarach wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń

i sieci telekomunikacyjnych,

h) **sieci rozległej** – należy przez to rozumieć siec publiczna w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z pózn. zm.).

II.Wyznaczenie Administratora Bezpieczeństwa Informacji.

1. Administrator Danych wyznaczył Administratora Bezpieczeństwa Informacji według Załącznika Nr 1.1 do niniejszego opracowania.
2. Na podstawie art. 36 ustęp 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) Administrator Bezpieczeństwa Informacji, nadzoruje przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1 ustawy o ochronie danych osobowych.
3. Osoba wyznaczona przez Administratora Danych zastępująca Administratora Bezpieczeństwa Informacji realizuje zadania Administratora Bezpieczeństwa Informacji i składa Administratorowi Bezpieczeństwa Informacji pisemna relacje z wykonywanych czynności oraz podejmowanych działań.

III.Obszar przetwarzania danych osobowych.

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe wyznacza Administrator Bezpieczeństwa Informacji według wzoru określonego w Załączniku Nr 1.2 do niniejszego opracowania.
2. Wyznaczony przez Administratora Bezpieczeństwa Informacji obszar przetwarzania danych osobowych zatwierdza Administrator Danych.

IV.Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym.

1. W skład systemu wchodzą:
   a) dokumentacja papierowa (korespondencja, wnioski, deklaracje, itd.)
   b) urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.
   c) wydruki komputerowe
2. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym prowadzi Administrator Bezpieczeństwa Informacji według wzoru określonego w Załączniku Nr 1.3

V. Struktury zbiorów danych osobowych oraz sposób przepływu danych.

Opisy struktur zbiorów danych osobowych oraz powiązań między zbiorami jak równie sposób przepływu danych pomiędzy poszczególnymi systemami prowadzi Administrator Bezpieczeństwa Informacji według wzoru określonego w Załączniku Nr 1.4.

VI. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A. Środki ochrony fizycznej.

1. Budynek Urzędu Gminy w Psarach, w którym zlokalizowany jest obszary przetwarzania danych osobowych musi być nadzorowany przez ochronę budynku całą dobę (zamykany po zakończeniu pracy).
2. Wszystkie pomieszczenia Urzędu Gminy w Psarach po zakończeniu pracy muszą być zamykane.
3. Urządzenia służące do przetwarzania danych osobowych muszą znajdować się w pomieszczeniach zabezpieczonych co najmniej zamkami patentowymi.
4. W pomieszczeniu serwerowi, w którym znajdują się serwery i urządzenia sieci komputerowej, winien być zainstalowany system kontroli dostępu, żaluzje antywłamaniowe oraz klimatyzacja.
5. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności kierownika działu.
6. Jeżeli zachodzi konieczność przebywania osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych bez nadzoru odnotowuje się ten fakt w oddzielnym rejestrze według wzoru określonego w Załączniku Nr 1.5 do niniejszego opracowania.
7. Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
8. W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
9. Do przebywania w pomieszczeniu serwerowni uprawnieni są: Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego, osoby odpowiedzialne za obsługę informatyczną Urzędu Gminy w Psarach oraz Kierownik

Urzędu.

10. Przebywanie w pomieszczeniu serwerowni osób trzecich (np. konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. 9, a w przypadku ich nieobecności – w obecności osoby pisemnie upoważnionej przez Kierownika Urzędu.

B. Środki sprzętowe, informatyczne i telekomunikacyjne.

1. Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający odczytanie treści danych osobowych (np. przy pomocy niszczarki dokumentów).
2. Urządzenia wchodzące w skład systemu informatycznego winny być podłączone do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej lokalnym lub centralnym UPS-em.
3. Sieć lokalna winna być podłączona do Internetu za pomocą odrębnego komputera lub urządzenia spełniającego funkcje Firewall'a (zapory ogniowej).
4. Należy stosować odpowiednie oprogramowanie do tworzenia kopii zapasowych.
5. Na wszystkich serwerach oraz stacjach roboczych należy zainstalować oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu Gminy w Psarach winna być skanowana programem antywirusowym przed przesłaniem jej do użytkownika.
6. Kopie awaryjne można wykonywać na nośnikach danych typu: CD / DVD / HDD. Kopie te należy zabezpieczyć przed dostępem osób nieupoważnionych, zniszczeniem lub kradzieżą.

C. Środki ochrony w ramach oprogramowania systemu.

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osób zajmujących się obsługa informatyczną Urzędu Gminy w Psarach.
2. Konfiguracja systemu może umożliwić użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3. System informatyczny musi pozwalać na zdefiniowanie odpowiednich praw dostępu do zasobów informatycznych systemu.
4. W sieciowym systemie operacyjnym należy zastosować mechanizm wymuszający okresową zmianę haseł dostępu do sieci.

D. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

1. Zastosować należy identyfikator i hasło dostępu do danych na poziomie aplikacji.
2. Dla każdego użytkownika systemu powinien być ustalony odrębny identyfikator.
3. Zdefiniować należy użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

E. Środki ochrony w ramach systemu użytkowego.

1. Zastosować należy wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
2. Komputer, z którego możliwy jest dostęp do danych osobowych należy zabezpieczyć hasłem uruchomieniowym.

F. Środki organizacyjne.

1. Wyznaczono Administratora Bezpieczeństwa Informacji, który przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia Kierownika Urzędu określającego zakres uprawnień pracownika.
2. Osoby upoważnione do przetwarzania danych osobowych winny być przed dopuszczeniem ich do pracy z tymi danymi szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
3. Prowadzona winna być ewidencja osób upoważnionych do przetwarzania danych osobowych.
4. Wprowadzono Instrukcje Zarządzania Systemem Informatycznym.
5. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.
6. Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu według Załącznika Nr 2.7 do Instrukcji Zarządzania Systemem Informatycznym.
7. Określono sposób postępowania z nośnikami informacji.

VII.System szkoleń.

Wprowadza się obowiązek szkoleń wstępnych i okresowych (co 2 lata) z zakresu ochrony danych osobowych oraz obowiązujących przepisów wewnętrznych w tym zakresie. Instrukcja szkolenia w zakresie bezpieczeństwa danych osobowych w systemie informatycznym znajduje się w Załączniku Nr 1.6 do niniejszego opracowania.

VIII.Znajomość Polityki Bezpieczeństwa Systemu Informatycznego.

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy Urzędu upoważnieni do przetwarzania danych osobowych w systemie informatycznym.

ZAŁĄCZNIK NR 1.1
DO POLITYKI BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
SYSTEMU INFORMATYCZNEGO

WYZNACZENIE

ADMINISTRATORA BEZPIECZENSTWA INFORMACJI

Na podstawie art. 36 ustep 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) z dniem 25 marca 2008 r. wyznacza się:

Pana

Piotra Gawrona

na ADMINISTRATORA BEZPIECZENSTWA INFORMACJI

1. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

2. Jednocześnie tracą uprawnienia Administratora Bezpieczeństwa Informacji osoby wcześniej wyznaczone do pełnienia tych obowiązków.

25.06.2008 r. .....

data i podpis
Administratora Danych

25.06.2008 r. Piotr Gawron

data i podpis
Administratora Bezpieczeństwa Informacji

ZAŁĄCZNIK NR 1.2
DO POLITYKI BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
SYSTEMU INFORMATYCZNEGO

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Określanie obszaru pomieszczeń, w którym przetwarzane są dane osobowe, powinno obejmować zarówno miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe).

Dane osobowe przetwarzane są w budynku przy ulicy: Malinowickiej 4 w Psarach.

Lp.	Nazwa zbioru danych osobowych	Pomieszczenia w których przetwarzane są dane osobowe	Działy przetwarzające zbiór	Uwagi
1.		wszystkie pokoje usytuowane na pierwszym i drugim piętrze oraz pomieszczenie archiwum na parterze i w podpiwniczeniu budynku.		

ZAŁĄCZNIK NR 1.3
DO POLITYKI BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
SYSTEMU INFORMATYCZNEGO

WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

Wykaz ten powinien zawierać informacje w zakresie precyzyjnej lokalizacji miejsca (budynek, pomieszczenie, nazwa komputera lub innego urządzenia np. macierzy dyskowej, biblioteki optycznej itp.), w których znajdują się zbiory danych osobowych przetwarzane na bieżąco oraz nazwy i lokalizacje programów (modułów programowych) używanych do ich przetwarzania.

Dane osobowe przetwarzane są w budynku przy ulicy: Malinowickiej 4 w Psarach.

Lp.	Nazwa zbioru danych osobowych	Nazwa programu zastosowanego do przetwarzania zbioru	Autor programu
1.		dig-Systemy BUDŻET	Agencja Komputerowa Tomasz Gawron
2.		dig-Systemy FINANSE	Agencja Komputerowa Tomasz Gawron
3.		dig-Systemy KADRY i PŁACE	Agencja Komputerowa Tomasz Gawron
4.		dig-Systemy ODPADY	Agencja Komputerowa Tomasz Gawron
5.		dig-Systemy WYMIAR PODATKU	Agencja Komputerowa Tomasz Gawron
6.		SEDziG System Ewidencji Działalności Gospodarczej	AS Zakład Systemów Komputerowych Andrzej Szepe
7.		KONCESJA Koncesja zezwolenia na sprzedaż napojów alkoholowych	AS Zakład Systemów Komputerowych Andrzej Szepe
8.		EWIDENCJA LUDNOŚCI	CLANET
9.		PŁATNIK	PROCOM
10.		PB_USC Komputerowy System Rejestracji Aktów Stanu Cywilnego	TECHNIKA Gliwice

ZAŁĄCZNIK NR 1.4
DO POLITYKI BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
SYSTEMU INFORMATYCZNEGO

STRUKTURY ZBIORÓW DANYCH OSOBOWYCH ORAZ SPOSÓB PRZEPŁYWU DANYCH.

Wykaz ten powinien zawierać opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

ZAŁĄCZNIK NR 1.5
DO POLITYKI BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
SYSTEMU INFORMATYCZNEGO

REJESTR OSÓB NIEUPOWAŻNIONYCH DO PRZEBYWANIA W POMIESZCZENIACH BEZ NADZORU TWORZĄCYCH OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Data	Godzina Wejścia	Godzina Wyjścia	Dane Personalne Osoby Nieupoważnionej
1.				

ZAŁĄCZNIK NR 1.6
DO POLITYKI BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
SYSTEMU INFORMATYCZNEGO

INSTRUKCJA SZKOLENIA W ZAKRESIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM

Wszyscy pracownicy zobowiązani są do ochrony tajemnic prawnie chronionych. Dlatego też wszyscy użytkownicy systemów informatycznych powinni być zapoznani ze znaczeniem bezpieczeństwa danych oraz systemów informatycznych. Przeszkolenie jest warunkiem koniecznym dopuszczenia pracownika do danych osobowych i ich przetwarzania. Osoby zatrudnione przy przetwarzaniu danych osobowych, mające do nich dostęp, są obowiązane do zachowania ich w tajemnicy (zarówno w czasie zatrudnienia, jak tez po jego ustaniu).

Konieczność zapoznania się i przestrzegania przepisów i zasad wymienionych w niniejszym dokumencie wynika z wejścia w życie ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z dnia 29 października 1997 r.), zwanej dalej ustawą i aktów wykonawczych.

W myśl ustawy:

Art. 1.1. Każdy ma prawo do ochrony dotyczących go danych osobowych.

Art. 2.2. Ustawę stosuje się do przetwarzania danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych.

DEFINICJE POJĘĆ

DANE OSOBOWE - w rozumieniu ustawy za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby. Będzie to np. imię, nazwisko, adres tej osoby, ale też jej PESEL lub NIP. Należy pamiętać, że są nimi także wszystkie informacje dotyczące konkretnej osoby, już zidentyfikowanej np. wysokość wynagrodzenia, obywatelstwo, numer rejestracyjny samochodu, numer rachunku bankowego, numer telefonu, wizerunek, stan konta bankowego.

ZBIÓR DANYCH OSOBOWYCH - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje). Należy przez to rozumieć, że zbiorem danych osobowych jest nie tylko komputerowa baza danych, ale także kartoteka, skorowidz, księga, wykaz, itp. zawierające dane o charakterze osobowym, tj. pozwalające ustalić tożsamość osób, które się w nich znajdują.

PRZETWARZANIE DANYCH OSOBOWYCH - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie które wykorzystuje się w systemach informatycznych. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- jest to niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą

SYSTEM INFORMATYCZNY - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

ADMINISTRATOR DANYCH OSOBOWYCH - to organ, instytucja, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI - jest osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO - 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.

GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH - w skrócie Generalny Inspektor (GIODO) - to organ ds. ochrony danych osobowych, powoływany i odwoływany przez Sejm Rzeczypospolitej za zgodą Senatu na 4 lata (ta sama osoba nie może być GIODO więcej niż przez dwie kadencje). GIODO nie może jednocześnie zajmować innego stanowiska, z wyjątkiem stanowiska profesora szkoły wyższej, ani wykonywać innych zajęć zawodowych, jak również nie może należeć do partii politycznej, związku zawodowego, ani prowadzić działalności publicznej, nie dającej się pogodzić z godnością jego urzędu. GIODO ma szerokie uprawnienia. Przysługuje mu prawo wstępu do pomieszczeń, w których przechowywany jest zarejestrowany zbiór danych i przeprowadzenia tam kontroli, czy dane przetwarzane są zgodnie z ustawą. Ponadto może przesłuchiwać osoby zatrudnione w tych firmach, żądać dokumentów i innych dowodów mających związek z kontrolą. W celu wykonania zadań Generalny Inspektor lub upoważnieni przez niego inspektorzy mają w szczególności prawo:

- wstępu w godz. od. 6.00 do 22.00, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczeń, w którym zlokalizowany jest zarejestrowany zbiór danych i przeprowadzenia czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
- żądać złożenia pisemnych lub ustnych wyjaśnień i wzywać oraz przesłuchiwać osoby w celu ustalenia stanu faktycznego,
- żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
- żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,
- zlecać sporządzanie ekspertyz i opinii.

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

ODBIORCA DANYCH - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby, upoważnionej do przetwarzania danych,
- przedstawiciela w Rzeczypospolitej Polskiej podmiotu. Który przetwarza dane osobowe w państwie trzecim
- podmiotu, o którym mowa w art. 31,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

PAŃSTWO TRZECIE - jest to państwo nienależące do Europejskiego Obszaru Gospodarczego

JEDNOSTKI I INSTYTUCJE OBJĘTE OCHRONĄ DANYCH OSOBOWYCH

- podmioty publiczne:
  - organy państwowe,
  - organy samorządu terytorialnego,
  - państwowe i komunalne jednostki organizacyjne,
  - podmioty prywatne realizujące zadania publiczne, decydujące o celach i środkach przetwarzania danych.
- podmioty prywatne:
  - osoby fizyczne prowadzące działalność gospodarczą,
  - spółki prawa handlowego,
  - spółki cywilne
  - spółdzielnie,
  - stowarzyszenia,

- kościoły i związki wyznaniowe, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub do realizacji celów statutowych.

ELEMENTY SYSTEMU INFORMATYCZNEGO PODLEGAJĄCE OCHRONIE

- sprzęt komputerowy i okablowanie,
- oprogramowanie,
- dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie,
- hasła użytkowników,
- pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa,
- użytkownicy i administratorzy, którzy obsługują i używają systemu,
- dokumentacja systemu,
- wydruki.

ZAGROŻENIA

Zagrożenie jest to potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub jednostki. Każda sytuacja która powoduje niedostępność danych (czasowe lub trwałe uniemożliwienie przetwarzania zbiorów danych), ich niekontrolowany wypływ, ujawnienie czy utratę lub przekłamanie - jest zagrożeniem systemu, niezależnie od tego czy jest to celowy sabotaż, czy przypadkowe zdarzenie.
Realne zagrożenia można podzielić na kilka podstawowych kategorii:

ZAGROŻENIE LOSOWE ZEWNĘTRZNE - (np. klęski żywiołowe, przerwy w zasilaniu); ich wystąpienie może prowadzić do utraty integralności danych, ich zniszczenia, a nawet do zniszczenia całej infrastruktury technicznej systemu; ciągłość systemu zostaje zakłócona, nie dochodzi zazwyczaj do naruszenia poufności danych;

ZAGROŻENIE LOSOWE WEWNĘTRZNE - (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania); ich wystąpienie również może prowadzić do utraty integralności danych, ich zniszczenia; może zostać zakłócona ciągłość pracy systemu, a w sytuacjach wyjątkowych może nastąpić naruszenie poufności danych;

ZAGROŻENIE ZAMIERZONE - czyli świadome i celowe - jest to najpoważniejszy rodzaj zagrożenia - naruszenie poufności danych; zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenia ciągłości pracy; zagrożenia takie można 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.

NARUSZENIE BEZPIECZEŃSTWA SYSTEMU

Wykrywaniem naruszeń bezpieczeństwa danych i systemów informatycznych nazywamy proces znajdowania i identyfikowania nieautoryzowanych lub niecodziennych zdarzeń w systemie. Można rozróżnić następujące sposoby wykrycia naruszenia bezpieczeństwa:

- złapanie sprawcy na gorącym uczynku,
- wnioskowanie na podstawie zmian w systemie,
- doniesienie np. od innego administratora,
- stwierdzenie zajścia niezwykłych zdarzeń.

Jeżeli użytkownik systemu informatycznego na podstawie takich czynników jak:

- stan urządzeń,
- zawartość zbioru danych osobowych,
- informacja o każdej nieuprawnionej próbie zmiany hasła,

- informacja o każdej nieuprawnionej próbie logowania do systemu,
- sposób działania programu,
- ujawnione metody pracy,
- własne doświadczenia osiągnięte w trakcie pracy z aplikacją komputerową itp.

nabędzie przypuszczeń lub stwierdzi fakt naruszenia bezpieczeństwa danych w systemie, wówczas zobowiązany jest do:

1) zabezpieczenia pomieszczenia, w którym znajduje się urządzenie informatyczne;
2) zawiadomienie o powyższym fakcie administratora bezpieczeństwa informacji lub inną upoważnioną przez niego osobę.

STREFA PRZETWARZANIA DANYCH OSOBOWYCH

Administrator danych określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
Przebywanie wewnątrz tego obszaru osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą administratora danych lub osoby przez niego upoważnionej.
Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

ROZPOCZĘCIE, WSTRZYMANIE I ZAKOŃCZENIE PRACY

Rejestrowanie użytkownika odbywa się obowiązkowo za każdym razem, gdy użytkownik rozpoczyna pracę w systemie. Polega na wprowadzeniu identyfikatora i objętego tajemnicą, znanego tylko użytkownikowi hasła, na podstawie, których system stwierdza tożsamość użytkownika. Po poprawnym wykonaniu logowania użytkownik może wykonywać wszystkie czynności, na jakie pozwalają przydzielone mu prawa dostępu.
Zabronione jest opuszczanie systemu użytkowego w sposób różny od ustalonej procedury zamknięcia systemu (np. poprzez wyłączenie zasilania, zresetowanie stanowiska)

Czynności przy rozpoczęciu pracy w systemie informatycznym:

- włączenie komputera i o ile pozwalają na to możliwości sprzętowe podanie hasła dostępu określonego w BIOS-ie,
- po załadowaniu systemu operacyjnego rejestracja w systemie sieciowym (podanie loginu i hasła dostępu do sieci),
- po pozytywnym przejściu procedury uwierzytelnienia uzyskanie dostępu do systemu operacyjnego a następnie do poszczególnych programów,
- uruchomienie systemu użytkowego przetwarzającego dane osobowe może nastąpić jedynie poprzez podanie identyfikatora i hasła przydzielonego użytkownikowi w danym systemie.

Czynności przy wstrzymaniu pracy w systemie informatycznym:

- należy wyrejestrować się z systemu użytkowego przetwarzającego dane osobowe obecnie używanego,
- zakończyć działanie systemu użytkowego poprzez poprawne zamknięcie,
- wylogować się z systemu operacyjnego,
- zabezpieczenie pomieszczenia w taki sposób aby osoby postronne nie miały dostępu do systemu komputerowego.

Czynności przy zakończeniu pracy w systemie informatycznym:

- po zakończonej pracy - wyrejestrowanie z używanego systemu użytkowego,
- zakończenie pracy systemu operacyjnego poprzez wybranie menu Start i wciśnięcie ikony zamknij system (wyłącz komputer),
- wyłączenie komputera oraz monitora.

OBOWIĄZKI PRACOWNIKÓW MAJĄCE NA CELU PRZECIWDZIAŁANIE ZAGROŻENIOM

1. **Przestrzeganie zasad zarządzania hasłami:**
   - hasła użytkowników należą do nich samych,
   - są one objęte tajemnicą i nikt poza właścicielami haseł nie może ich znać,
   - hasło musi być zmieniane przez użytkownika nie rzadziej niż raz w miesiącu,
   - odpowiedzialność za okresowe zmiany hasła ciąży na użytkowniku - właścicielu hasła,
   - niedopuszczalne jest zapisywanie haseł (karteczki w biurku, nalepki na monitorach, itp.).

2. **Stosowanie się do zakazu:**
   - samowolnego instalowania i używania jakiegokolwiek oprogramowania (wliczając w to poprawki systemowe, freeware, shareware, itp),
   - trwałego lub czasowego kopiowania programów komputerowych w całości lub w części,
   - rozpowszechniania programów lub ich kopii,
   - przenoszenia sprzętu komputerowego oraz oprogramowania pomiędzy stanowiskami komputerowymi,
   - udostępniania osobom postronnym programów komputerowych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu.

3. **Przestrzeganie reguł prawidłowego rozpoczęcia, wstrzymania i zakończenia pracy z systemem informatycznym.**

4. **Zgłaszanie wszystkich wątpliwości i pytań Administratorowi Bezpieczeństwa Informacji związanych z:**
   - niepoprawnym działaniem sprzętu komputerowego,
   - niepoprawnym funkcjonowaniem aplikacji użytkowych,
   - podejrzeniem zainfekowania wirusem lub inną modyfikacją systemu,
   - jakością komunikacji w sieci komputerowej (gwałtowne opóźnienie lub przyspieszenie)
   - inną nie wymienioną sytuacją, a mogącą wskazywać na działanie osób trzecich.

ODPOWIEDZIALNOŚĆ KARNA

Przepisy o odpowiedzialności karnej wynikają z ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z dnia 29 października 1997r).

- Art. 49.
  - 1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
  - 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
- Art. 50. Kto administrując zbiorem danych przechowuje w zbiorze dane osobowe niezgodnie z celem utworzenia zbioru, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

- Art. 51.
  - 1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
  - 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- Art. 52. Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- Art. 53. Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- Art. 54. Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, ojej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

PODSTAWY PRAWNE

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z dnia 29 października 1997 r., Nr 133 póz. 883),
- 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 (Dz. U. z dnia 1 maja 2004r., Nr 100 póz. 1024).

Jeśli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z Ustawy o ochronie danych osobowych, stosuje się przepisy tych ustaw.

Załącznik Nr 2
do Zarządzenia Nr 0152/30/2008
Wójta Gminy Psary z dnia 25.06.2008 r.
w sprawie: Instrukcji Zarządzania Systemem Informatycznym Urzędu Gminy w Psarach

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY w PSARACH

Podstawa prawna:

- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)
- ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z pózn. zm.)

I. Definicje.

Ilekroć w niniejszym dokumencie jest mowa o:

a) **Urzędzie** – należy przez to rozumieć Urząd Gminy Psary,

b) **Kierowniku Urzędu** – należy przez to rozumieć Wójta Gminy Psary,

c) **Administratorze Danych** – należy przez to rozumieć Wójta Gminy Psary,

d) **Administratorze Bezpieczeństwa Informacji** – należy przez to rozumieć pracownika Urzędu Gminy w Psarach lub inną osobę wyznaczona do nadzorowania przestrzegania zasad ochrony danych osobowych ustanowionego zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu Gminy w Psarach,

e) **Administratorze Systemu Informatycznego** – należy przez to rozumieć osobę odpowiedzialna za funkcjonowanie systemu informatycznego Urzędu Gminy w Psarach oraz stosowanie technicznych i organizacyjnych środków ochrony,

f) **użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy w Psarach. Użytkownikiem może być pracownik Urzędu Gminy w Psarach, osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno - prawnej, osoba odbywająca staż lub praktykę w Urzędu Gminy w Psarach,

g) **sieci lokalnej** – należy przez to rozumieć połączenie systemów informatycznych Urzędu Gminy w Psarach wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

h) **sieci rozległej** – należy przez to rozumieć siec publiczna w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z pózn. zm.).

II. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych w systemie informatycznym musi zapoznać się z zasadami dotyczącymi Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędu Gminy w Psarach.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik Nr 2.2.
3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi Załącznik Nr 2.1.
4. Jedynie prawidłowo wypełniony wniosek o nadanie uprawnień w systemie oraz zmianę tych uprawnień jest podstawa rejestracji uprawnień w systemie.
5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
6. Hasło podane podczas przyznawania uprawnień przez Administratora Systemu Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym. Ustanowione hasło, Administrator Systemu Informatycznego przekazuje użytkownikowi ustnie.
7. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
8. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
9. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
10. Pracownik zobowiązany jest do zachowania ich w tajemnicy, traktowanej jako tajemnice służbowa. Tajemnica obowiązuje go równie po ustaniu zatrudnienia.
11. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
12. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
13. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
14. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.

15. Identyfikator osoby, która utraciła uprawnienia dostępu należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
16. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.
17. Rejestr, którego wzór stanowi Załącznik Nr 2.3, powinien zawierać:
    a) identyfikator użytkownika,
    b) imię i nazwisko użytkownika systemów informatycznych,
    c) rodzaj i zakres uprawnienia,
    d) datę nadania uprawnienia,
    e) datę odebrania uprawnienia,
    f) przyczynę odebrania uprawnienia,
    g) podpis Administratora Bezpieczeństwa Informacji.
18. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

III. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika jest zmieniane co najmniej raz w miesiącu.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy równie po upływie ich ważności.
6. Pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
9. Przy wyborze hasła obowiązują następujące zasady:
    a) minimalna długość hasła - 8 znaków,
    b) zakazuje się stosować:
        - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
        - swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),

- swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
- imion (w szczególności imion osób z najbliższej rodziny),
- ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
- wyrazów słownikowych,
- przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.

c) należy stosować:

- hasła zawierające kombinacje liter i cyfr,
- hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala,
- hasła, które można zapamiętać bez zapisywania,
- hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,

10. Zmiany hasła nie wolno zlecać innym osobom.
11. W systemach, które umożliwiają opcje zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
12. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
    a) Administrator Bezpieczeństwa Informacji,
    b) Kierownik Urzędu lub osoba przez niego wyznaczona.

IV. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwacje należy wykonać opcje wymeldowania z systemu (zablokowania dostępu), lub jeśli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcje wymeldowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamkniecie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej.

5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

V. Procedury tworzenia zabezpieczeń.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego, a w przypadku jego nieobecności Administrator Bezpieczeństwa Informacji lub osoba wyznaczona przez Administratora Danych.
2. Administrator Bezpieczeństwa Informacji nadzoruje oraz kontroluje sposób tworzenia i przechowywania kopii bezpieczeństwa.
3. Kopie bezpieczeństwa wykonywane są raz w tygodniu po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
4. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest raz do roku w postaci zapisu na płytach CD / DVD,
5. Płyty CD / DVD przechowuje się w kasie pancernej Urzędu Gminy w Psarach.
6. Płyty CD / DVD należy raz do roku sprawdzić pod kątem ich dalszej przydatności.

VI.Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

A. Elektroniczne nośniki informacji.

1. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa – zapisane na dyskietkach, dyskach magnetooptycznych, dyskach twardych, itp., nie są wynoszone poza siedzibę Urzędu Gminy w Psarach.
2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych Urzędu Gminy w Psarach.
3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w kasach pancernych, zamykanych szafach biurowych lub kasetkach.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do

otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.

6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora Danych.

B. Kopie zapasowe.

1. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w kasie pancernej w Urzędzie Gminy w Psarach.
2. Dostęp do danych opisanych w punkcie 1 ma Administrator Bezpieczeństwa Informacji i Administrator Systemu Informatycznego oraz upoważnieni przez Administratora Danych pracownicy.

C. Wydruki.

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

VII.Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi.

1. Na Każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do Urzędu Gminy w Psarach musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusowa.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w tygodniu.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.

6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum co trzy miesiące.
8. Kontrola antywirusowa przeprowadzana jest równie na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki zewnętrzne.

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

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.
4. Udostępnienie danych osobowych może nastąpić wyłącznie po przedstawieniu wniosku, którego wzór stanowi Załącznik Nr 2.4 do niniejszej instrukcji.
5. Kierownicy komórek organizacyjnych prowadzą rejestry udostępnionych danych osobowych według wzoru do Załącznika Nr 2.5 niniejszego opracowania.
6. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji udzielonych odbiorcom danych. Zakres informacji powinien obejmować, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

IX.Sposób postępowania w sytuacji naruszenia ochrony danych osobowych.

Sposób postępowania w sytuacji stwierdzenia naruszenia ochrony danych osobowych określa Załącznik Nr 2.6 do niniejszej instrukcji.

X. Procedury wykonywania przeglądów i konserwacji systemu.

A. Przeglądy i konserwacja urządzeń.

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu.
2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

B. Przegląd programów i narzędzi programowych.

1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
2. Administrator Systemu Informatycznego zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcje.
3. Wszystkie logi opisujące prace systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy archiwizować.

C. Rejestracja działań konserwacyjnych, awarii oraz napraw.

1. Administrator Bezpieczeństwa Informacji prowadzi „Dziennik Systemu Informatycznego". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w Załączniku Nr 2.7.
2. Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego lub osoby przez nich wyznaczone.

XI.Połączenie do sieci Internet.

1. Połączenie lokalnej sieci komputerowej Urzędu Gminy w Psarach z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych (firewall) oraz kompleksowego oprogramowania antywirusowego.

XI.Użytkowanie komputerów przenośnych.

1. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególna ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych oraz zabezpiecza komputer hasłem uruchomieniowym.

ZAŁACZNIK NR 2.1.
DO INSTRUKCJI ZARZADZANIA
SYSTEMEM INFORMATYCZNYM

WNIOSEK O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

.....

wpisać nazwę systemu

Nowy użytkownik ☐	Modyfikacja uprawnień ☐	Odebranie uprawnień ☐

Imię i nazwisko użytkownika:	Dział	Stanowisko
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:		
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika	
Data zaopiniowania:	Opinia i podpis Właściciela Informacji (tylko jeśli nie jest to bezpośredni przełożony użytkownika)	
Data zaopiniowania:	Opinia i podpis Administratora Bezpieczeństwa Informacji	
Data decyzji:	Zgoda Administratora Danych poświadczona podpisem	
Data realizacji:	Potwierdzenie nadania (odebrania) uprawnień w systemie przez Administratora Systemu Informatycznego	
Data odbioru:	Potwierdzenie odbioru uprawnień przez pracownika	

Okres obowiązywania zgody na dostęp do danych:

bezterminowo ☐ na okres od ..... do .....

ZAŁACZNIK NR 2.2.
DO INSTRUKCJI ZARZADZANIA
SYSTEMEM INFORMATYCZNYM

....., dnia .....
miejscowość

.....
(nazwisko i imię)

.....
(referat)

.....
(stanowisko)

ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI
ORAZ OŚWIADCZENIE O ZNAJOMOŚCI ZASAD POLITYKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Zobowiązuje się do bezwzględnego zachowania w poufności, także po zakończeniu pracy / praktyki / stażu, wszelkich informacji uzyskanych w związku z odbywaniem praktyki lub stażu w Urzędu Gminy w Psarach. Obowiązek ten dotyczy wszelkich informacji dotyczących Urzędu Gminy w Psarach, które nie są opublikowane do publicznej wiadomości.

Niniejszym oświadczam, że zapoznałem się z obowiązującymi mnie podczas pracy / praktyki / stażu w Urzędu Gminy w Psarach, zasadami zawartymi w dokumentacji „Polityka Bezpieczeństwa Przetwarzania Danych Osobowych" i zobowiązuje się do ich przestrzegania.

Przyjmuje do wiadomości, że przez obowiązek bezwzględnego zachowania w poufności rozumie się w szczególności zakaz:

- zapoznawania się przez pracownika / praktykanta / stażystę z dokumentami, analizami, zawartością dysków twardych i innych nośników informacji itp. – nie związanymi z jego zakresem prac,
- kopiowania oraz powielania dokumentów i danych bez zgody przełożonego, a w szczególności udostępniania ich osobom trzecim,
- informowania osób trzecich w zakresie spraw objętych nakazem poufności.

Przyjmuje do wiadomości, że naruszenie zasady poufności lub zasad Polityki Bezpieczeństwa Informacji, obowiązującego w Urzędu Gminy w Psarach, może spowodować wobec mnie odpowiedzialność dyscyplinarną, karną lub sankcje finansowe.

.....
(podpis pracownika)

ZAŁACZNIK NR 2.3.
DO INSTRUKCJI ZARZADZANIA
SYSTEMEM INFORMATYCZNYM

REJESTR UŻYTKOWNIKÓW I UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

KARTA EWIDENCYJNA UPRAWNIEŃ OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM

Identyfikator użytkownika	Nazwisko i Imię

Lp.	Nazwa systemu	Zakres upoważnienia	Identyfikator systemowy użytkownika (login name)	Data nadania uprawnień	Podpis osoby upoważnionej	Data i przyczyna odebrania uprawnień
1.						

ZAŁĄCZNIK NR 2.4
DO INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

WNIOSEK

O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do Wójta Gminy Psary

2. Wnioskodawca

.....

.....

(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. 29 ust. 1 ustawy o ochronie danych osobowych:

.....

..... ☐* ew. cd. w załączniku nr. .....

4. Wskazanie przeznaczenia dla udostępnionych danych:

.....

..... ☐* ew. cd. w załączniku nr. .....

5. Oznaczenie lub nazwa zbioru, z którego maja być udostępnione dane:

.....

.....

6. Zakres żądanych informacji ze zbioru:

.....

..... ☐* ew. cd. w załączniku nr. .....

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych:

.....

..... ☐* ew. cd. w załączniku nr. .....

---

* Jeżeli TAK, to zakreślać kwadrat litera „X":

(miejsce na znaczki opłaty skarbowej)

.....

(data, podpis i ew. pieczęć wnioskodawcy)

ZAŁACZNIK NR 2.5.
DO INSTRUKCJI ZARZADZANIA
SYSTEMEM INFORMATYCZNYM

REJESTR UDOSTĘPNIONYCH DANYCH OSOBOWYCH

Lp.	Data Udostępnienia Informacji	Podstawa Prawna	Zakres Udostępnionych Informacji	Osoba lub Instytucja
1.				

ZAŁACZNIK NR 2.6.
DO INSTRUKCJI ZARZADZANIA
SYSTEMEM INFORMATYCZNYM

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejsza instrukcja reguluje postępowanie pracowników Urzędu Gminy w Psarach zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych (Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych).

§ 1.

Celem niniejszej instrukcji jest określenie zadań pracowników w zakresie:

1. Ochrony danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem, ujawnieniem lub pozyskaniem danych osobowych, a także ich utrata oraz ochrona zasobów technicznych,
2. Prawidłowego reagowania pracowników zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia ochrony danych osobowych lub zabezpieczeń systemu informatycznego.

§ 2.

Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:

1. Stanu urządzeń technicznych,
2. Zawartości zbiorów danych osobowych,
3. Sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej,
4. Metod pracy (w tym obiegu dokumentów).

§ 3.

W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie:

1. Powiadomić Administratora Bezpieczeństwa Informacji lub bezpośredniego przełożonego lub Kierownika Urzędu,
2. Zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych,
3. Podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie

powstałego zagrożenia - o ile czynności te nie spowodują przekroczenia uprawnień pracownika,

4. zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.

§ 4.

1. Bezpośredni przełożony pracownika po otrzymaniu powiadomienia o naruszenia bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub Kierownika Urzędu, chyba, że zrobił to pracownik, który stwierdził naruszenie.
2. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych Administrator Bezpieczeństwa Informacji i osoba przełożona pracownika przejmują nadzór nad praca w systemie odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.

§ 5.

Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona podejmuje czynności wyjaśniające mające na celu ustalenie:

1. Przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych,
2. Osób winnych naruszenia bezpieczeństwa danych osobowych,
3. Skutków naruszenia.

§ 6.

1. Administrator Bezpieczeństwa Informacji zobowiązany jest do powiadomienia o zaistniałej sytuacji Kierownika Urzędu, który podejmuje decyzje o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego co najmniej:
   a) datę i miejsce wystąpienia naruszenia,
   b) zakres ujawnionych danych,
   c) przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy,
   d) sposób rozwiązania problemu,
   e) przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Raport ten Administrator Bezpieczeństwa Informacji przekazuje Kierownikowi Urzędu.

§ 7.

Za naruszanie ochrony danych osobowych obowiązują następujące kary wynikające m. in. z rozdziału 8 ustawy o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z pózn. zm.):

1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli czyn określony w pkt. 1 dotyczy danych tzw. wrażliwych (danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjna lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym) sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
3. Kto będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawiania wolności do lat 2.
4. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do roku.
5. Kto narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
6. Za naruszenie ochrony danych osobowych Kierownik Urzędu może stosować kary porządkowe, niezależnie od zastosowania kar, o których mowa wyżej.

ZAŁACZNIK NR 2.7.
DO INSTRUKCJI ZARZADZANIA
SYSTEMEM INFORMATYCZNYM

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:

- w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu – opis podjętych działań, wnioski

DZIENNIK SYSTEMU INFORMATYCZNEGO

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania / wnioski	Podpis
1.				

Strona .....

Załącznik Nr 3
do Zarządzenia Nr 0152/30/2008
Wójta Gminy Psary z dnia 25.06.2008 r.
Wzór Ewidencji Osób Zatrudnionych Przy Przetwarzaniu
Danych Osobowych w Urzędzie Gminy Psary

Wzór Ewidencji Osób Zatrudnionych Przy Przetwarzaniu Danych Osobowych w Urzędzie Gminy Psary

LP	Imię	Nazwisko	Data Nadania	Data Ustania	Zakres Upoważnienia	Identyfikator (Login)	Podpis

Załącznik Nr 4
do Zarządzenia Nr 0152/30/2008
Wójta Gminy Psary z dnia 25.06.2008 r.
Wzór Upoważnienia Do Przetwarzania
Danych Osobowych w Urzędzie Gminy Psary

Wzór Upoważnienia Do Przetwarzania Danych Osobowych w Urzędzie Gminy Psary

Psary, dnia .....

PP.0305/.....

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) u p o w a ż n i a m:

Panią/Pana ..... (PESEL: .....)

zatrudnioną w Urzędzie Gminy w Psarach

do przetwarzania danych i obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w zakresie aktualnie zajmowanego stanowiska pracy oraz odrębnie ustalonych zastępstw na czas nieobecności pracownika w pracy.

.....

(podpis i pieczęć administratora danych)