

*Załącznik Nr 1 Polityki bezpieczeństwa i instrukcja zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych w urzędzie Gminy Imielno*

(WZÓR)

.....
(pieczęć)

....., dnia r.

UPOWAŻNIENIE NR

z dnia

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) upoważniam Panią/a

..... zatrudnioną/ego w
..... na stanowisku
..... do przetwarzania danych
osobowych.

Zadania i czynności do wykonania:

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawą o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).
2. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym. (Rozdział VI)
3. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych. (Rozdział VII)
4. Przestrzeganie zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienia w związku z upoważnieniem do przetwarzania danych osobowych, także po ustaniu stosunku pracy.
5. W szczególności przetwarzanie danych osobowych w następujących zbiorach danych (numer i nazwa):

.....
(data i podpis Administratora Danych Osobowych)

.....
(data i podpis pracownika)

.....
(imię i nazwisko)

.....
(referat)

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 ze zm.) oraz rozporządzeniem ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz. U Nr 100, poz. 1024) i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Imielno wprowadzoną zarządzeniem nr Wójta Gminy Imielno z dnia

..... r. oraz Instrukcją przetwarzania danych osobowych. Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w:

*Urząd Gminy Imielno
ul. Cmentarna 7
28-313 Imielno*

Otrzymałem(łam) dnia:

.....
(podpis pracownika)

....., dnia r.

WYCOFANIE UPOWAŻNIENIA

Na podstawie art.37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 ze zm.) w związku z:

.....
.....
.....

cofam upoważnienie

Pana/Pani

.....
zatrudnionego/zatrudnionej w na
stanowisku.....
do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

.....
(data i podpis Administratora Danych Osobowych)

Otrzymałem(łam) dnia:

.....
(podpis pracownika)

....., dnia r.

**Wykaz pomieszczeń lub części pomieszczeń w których
przetwarzane są dane**

Lp.	Nr pokoju	Referat/Sam. Stanowisko (imię i nazwisko)	Określenie części pomieszczenia, w którym przetwarza się, lub archiwizuje dane.
1			
2			
3			
4			
5			
6			
7			
8			
9			

Wykaz zbiorów przetwarzanych elektronicznie

Lp.	Nr pokoju	Referat/Sam. Stanowisko (imię i nazwisko)	Nazwa urządzenia i program zainstalowany do przetwarzania (urządzenie/system/program/wersja)	Nazwa zbioru/Cel przetwarzania
1				
2				
3				
4				
5				
6				
7				
8				
9				

Wykaz zbiorów przetwarzanych w inny sposób niż elektronicznie

Lp.	Nr pokoju	Referat/Sam. Stanowisko (imię i nazwisko)	Rodzaj danych/Cel przetwarzania	Nazwa zbioru
1				
2				
3				
4				
5				
6				
7				
8				
9				

Opis struktury zbiorów danych

Zgodnie z §4 pkt 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024), dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane.

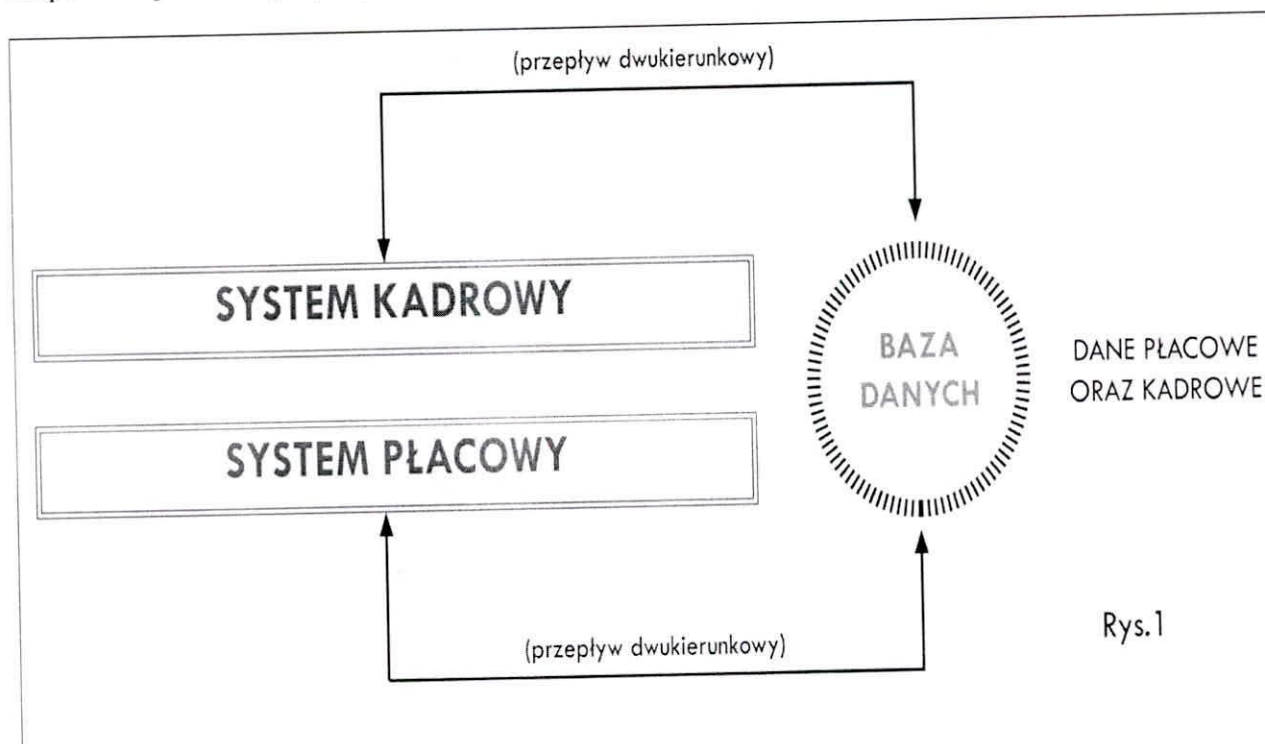
W §4 pkt 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024) wyraźnie wskazano, że w polityce bezpieczeństwa ma być zawarty opis struktury zbiorów wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. Opis ten może być przedstawiony w postaci formalnej, w postaci graficznej pokazującej istniejące powiązania pomiędzy obiektami, jak również opisu tekstowego. Opis struktury zbioru danych powinien znajdować się w dokumentacji technicznej eksploatowanych systemów. Dokumentacja może być załączona w formie elektronicznej lub papierowej.

Załączniki:

1. _____
2. _____
3. _____
4. _____

Sposób przepływu danych pomiędzy systemami

1. W Urzędzie Gminy Imielno istnieją relacje pomiędzy różnymi systemami informatycznymi i należy przedstawić w tym załączniku sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach do przetwarzania, których systemy te są wykorzystywane. Przedstawiając przepływ danych można posłużyć się np. schematami, jak na rys. 1, które wskazują, z jakimi zbiorami dany system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest jednokierunkowy, np. informacje pobierane są tylko do odczytu, czy dwukierunkowy (do odczytu i do zapisu). W sposobie przepływu danych pomiędzy poszczególnymi systemami należy zamieścić również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych), lub półautomatycznie - za pomocą teletransmisji (przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu.



Opis rejestracji baz danych

W przypadku konieczności przetwarzania danych w nowej bazie danych, wymagana jest konsultacja z Administratorem Bezpieczeństwa Informacji (ABI). W przypadku konieczności rejestracji bazy danych w **Generalnym Inspektoracie Danych Osobowych**, rejestracja następuje na wniosek danego referatu.

Każdy referat powinien prowadzić dokumentację opisującą bazy danych osobowych przetwarzanych w wydziale.

Dokumentacja winna zawierać:

- a. nazwę bazy,
- b. imię i nazwisko osoby tworzącej,
- c. datę utworzenia,
- d. ewentualną datę zakończenia przetwarzania danych,
- e. podstawę prawną przetwarzania,
- f. cel przetwarzania,
- g. listę osób przetwarzających dane,
- h. zakres danych osobowych zawartych w bazie,
- i. przewidywany czas użytkowania bazy (stały, okresowy, jednorazowy),
- j. informacje o ewentualnym przekazywaniu danych (komu, kiedy, w jakim celu, pod stawą prawną, jaki zakres przekazania danych),
- k. dodatkowe ważne informacje (zmiany osób uprawnionych itp.).

Opis zabezpieczeń systemów informatycznych

1. W celu ochrony przed **utratą danych** w Urzędzie Gminy Imielno stosowane są następujące zabezpieczenia:

- a. odrębne zasilanie sprzętu komputerowego,
- b. ochrona serwerów przed zanikiem (wahaniami) zasilania poprzez stosowanie zasilaczy zapasowych UPS,
- c. ochrona newralgicznych elementów sieciowych (switchy) przed zanikiem zasilania,
- d. ochrona przed utratą zgromadzonych danych przez robienie codziennych kopii zapasowych na taśmach magnetycznych, dyskach przenośnych lub płytach CD/DVD, z których w przypadku awarii odtwarzane są dane i system operacyjny,
- e. ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych (mirroring),

Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych, a nawet zatrzymania pracy systemu (zastosowanie elementów hotswap i hotspare).

2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu Gminy Imielno:

- a. wszystkie gniazda lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (zkrosowanie) danego użytkownika do szkieletu sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji, lub **ASI**,
- b. aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie mają być udostępnione,

- c. w systemie informatycznym Urzędu Gminy Imielno zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Urzędu podając login oraz hasło, drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika oraz hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.

3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu Gminy poprzez Internet.

W zakresie dostępu do sieci wewnętrznej Urzędu Gminy z rozległej sieci Internet zastosowano środki ochrony przed podsłuchiwaniami, penetrowaniem i atakiem z zewnątrz.

Zastosowano firewall na routerze, który ma za zadanie uwierzytelnianie źródła przychodzących pakietów oraz ich filtrowanie w oparciu o adres IP i inne parametry. Zablokowano wszystkie nieużywane porty celem zmniejszenia potencjalnych luk, które mogą być wykorzystane przez osobę próbującą uzyskać nieautoryzowany dostęp do sieci wewnętrznej. Ruch pakietów, oraz otwarte porty zostały określone przez Administratora Bezpieczeństwa.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez router. dostęp do sieci zewnętrznej jest ustalony indywidualnie na wniosek pisemny, lub ustny użytkownika. Oprócz filtra pakietów (firewall) zastosowano system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

- a. zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wszystkich zbędnych portów,
- b. objęcie ochroną antywirusową wszystkich danych ściąganych z sieci Internet na stacjach lokalnych,
- c. zapisywanie do logów połączeń użytkowników z siecią Internet.

4. Postanowienia końcowe.

- a. do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami, lub aplikacjami. Dostęp ten powinien być kontrolowany za pomocą drzwi z elektronicznym zamkiem szyfrowym,
- b. zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez ABI zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
- c. osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytych szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r.,
- d. w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewni właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
- e. w pobliżu wejścia do pomieszczenia z serwerami i innymi urządzeniami powinna znajdować się gaśnica, która jest okresowo napełniana i kontrolowana przez stosownego specjalistę.

**Raport nr/.....
z naruszenia bezpieczeństwa systemu informatycznego
w Urzędzie Gminy Imielno**

Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

Osoba przyjmująca zgłoszenie o zaistniałym zdarzeniu:

.....
(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

Lokalizacja zdarzenia:

.....
(np. nr pokoju; nazwa pomieszczenia)

Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące:

Podjęte działania:

Przyczyny wystąpienia zdarzenia:

Postępowanie wyjaśniające:

Ocena skuteczności przeprowadzonego postępowania naprawczego:

Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnym naruszeniom ochrony danych osobowych:

.....

.....

.....

.....
(data, podpis Administratora Bezpieczeństwa Informacji)

(WZÓR)

**Wzór wykazu osób które zapoznały się z „Polityką bezpieczeństwa
systemów informatycznych służących do przetwarzania danych
osobowych w Urzędzie Gminy Imielno.”**

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych
służących do przetwarzania danych osobowych w Urzędzie Gminy Imielno”, przeznaczonej dla
osób zatrudnionych przy przetwarzaniu tych danych.

Nr upoważnienia	Nazwisko I Imię	Data nadania	Upoważniający	Data odebrania	Odbierający
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					

.....
(data, podpis Administratora Bezpieczeństwa Informacji)

Ewidencja osób upoważnionych do przetwarzania danych.

	Imię	Nazwisko	Identyfikator
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			

.....
(data, podpis Administratora Bezpieczeństwa Informacji)