**POLITYKA BEZPIECZEŃSTWA**

Administrator Danych.....................................................................................................

Dnia .................................... w podmiocie o nazwie .............................................

Zgodnie z **ROZPORZĄDZENIEM 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)**

wdraża dokument o nazwie „Polityka Bezpieczeństwa”. Zapisy tego dokumentu wchodzą w życie   
z dniem............................................

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w …………………………………….. (nazwa podmiotu), określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych.

Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa” jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę,   
   o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,
7. administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.
8. podmiocie – rozumie się przez to firmę, instytucję,

§ 3.

Administrator Danych w podmiocie................................................................wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa  
w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Upoważnienie dla **Administratora Bezpieczeństwa Informacji** oraz zakres obowiązków określa **załącznik do „Polityki Bezpieczeństwa” nr 1**

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa” nr 2**

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik do „Polityki Bezpieczeństwa” nr 3**

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik  
do „Polityki Bezpieczeństwa” nr 4**

§ 7.

**Administratora Bezpieczeństwa Informacji** dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych** lub **Administratora Bezpieczeństwa Informacji**. **Administrator Bezpieczeństwa Informacji** jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,  
a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Bezpieczeństwa Informacji nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa”**. Administrator Bezpieczeństwa Informacji prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 6** do „Polityki Bezpieczeństwa”
2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu  
   są przekazywane. – **załącznik nr 7** do „Polityki Bezpieczeństwa”

§ 9.

Na wniosek osoby, której dane dotyczą, Administrator Bezpieczeństwa Informacji jest obowiązany,  
w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator Bezpieczeństwa Informacji może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten,  
może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa” mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI** z dnia 29 kwietnia 2004 r. **w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych**

Podpis Administratora Danych Osobowych

….....................................................................

Podpis

Podpis Administratora Bezpieczeństwa Informacji

….....................................................................

Podpis