Załącznik Nr 1
do Zarządzenia Nr 58 /2011
Wójta Gminy Śniadowo
z dnia 08 września 2011r.

POLITYKA BEZPIECZEŃSTWA

§1.
Postanowienia ogólne

1. Niniejsza „Polityka Bezpieczeństwa", zwana dalej Polityką została opracowana zgodnie z wymaganiami § 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) .

2. Ilekroć w niniejszym dokumencie jest mowa o:

   1) **Ustawie** – należy przez to rozumieć - ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
   2) **Urzędzie** – należy przez to rozumieć - Urząd Gminy Śniadowo z siedzibą w Śniadowie, ul. Ostrołęcka 11, Zakład Gospodarki Komunalnej w Śniadowie z siedzibą przy ul. Ostrołęckiej 11, Gminny Ośrodek Kultury w Śniadowie z siedzibą przy ul. Ostrołęckiej 13 i Bibliotekę Publiczną w Śniadowie z siedzibą przy ul. Ostrołęckiej 7,
   3) **Administratorze Danych (ADO)**- należy przez to rozumieć Wójta Gminy Śniadowo,
   4) **Administratorze Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych (Wójta) do nadzorowania przestrzegania zasad ochrony danych osobowych oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w Urzędzie Gminy Śniadowo, powołanego zarządzeniem Wójta Gminy Śniadowo,
   5) **Użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w urzędzie na podstawie stosunku pracy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej, umowy cywilno-prawnej, osoba odbywająca staż w urzędzie,
   6) **Identyfikatorze użytkownika** – należy przez to rozumieć ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
   7) **Administratorze Systemu Informatycznego (ASI)** – należy przez to rozumieć pracownika odpowiedzialnego za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie, powołanego zarządzeniem Wójta Gminy Śniadowo,

8) **Sieci lokalnej** – należy przez to rozumieć połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,
9) **Sieci telekomunikacyjnej** – należy przez to rozumieć systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z poźn. zm.),
10) **Publicznej sieci telekomunikacyjnej** - należy przez to rozumieć sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z poźn. zm.),
11) **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
12) **Przetwarzaniu danych** – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
13) **Zabezpieczeniu danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
14) **Telekomunikacji** – należy przez to rozumieć nadawanie, odbiór lub transmisję informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną,
15) **Aplikacji** – należy przez to rozumieć program komputerowy wykonujący konkretne zadanie,
16) **Komórce organizacyjnej** – należy przez to rozumieć gminne jednostki organizacyjna (GOK, ZGK, Biblioteka) referaty, samodzielne stanowiska pracy.

§2.
Cel i zakres Polityki Bezpieczeństwa

1. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów.
2. Polityka dotyczy wszystkich danych osobowych przetwarzanych w urzędzie niezależnie od formy ich przetwarzania oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
3. Celem Polityki jest ochrona danych osobowych przetwarzanych w Urzędzie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.
4. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   1) poufności – właściwości zapewniającej, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
   2) integralności – właściwości zapewniającej, że dane nie zostały zmienione lub

zniszczone w sposób nieautoryzowany;

3) rozliczalności – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

5. Za podmiot nieupoważniony uważa się podmiot, który nie otrzymał zgody ADO na udostępnienie mu danych osobowych w trybie i na zasadach określonych w art. 29 Ustawy oraz osobę nieposiadającą upoważnienia do przetwarzania danych osobowych, nadanego przez ADO w trybie art. 37 Ustawy.

6. Dla skutecznej realizacji Polityki ADO zapewnia:
1) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne;
2) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
3) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych;
4) kontrolę i nadzór nad przetwarzaniem danych osobowych;
5) monitorowanie zastosowanych środków ochrony.

§3.
Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Zarządzanie bezpieczeństwem systemów jest procesem ciągłym, realizowanym przy współdziałaniu użytkowników z ABI i ASI.

2. Wszystkie osoby przetwarzające dane osobowe zobowiązane są do:

1) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa;

2) postępowania zgodnie z ustaloną przez ADO „Polityką bezpieczeństwa" oraz z „Instrukcją zarządzania systemem informatycznym".

3. W przypadku naruszenia przepisów lub zasad postępowania użytkownik podlega odpowiedzialności służbowej i karnej.

4. Obowiązkiem ABI jest zapoznanie osób z procedurami i dokumentami związanymi z przetwarzaniem danych osobowych. Osoby, które zapoznały się z dokumentacją potwierdzają to podpisem w wykazie zamieszczonym w załączniku nr 3.

5. Kontrola i nadzór przestrzegania zasad bezpieczeństwa i ochrony danych osobowych określonych w dokumentacji, o której mowa w ust.2, należy do obowiązków ABI.

6. Użytkownicy systemu obowiązani są do:

1) ścisłego przestrzegania zakresu nadanego upoważnienia;

2) przetwarzania i ochrony danych osobowych zgodnie z przepisami;

3) zachowania w tajemnicy danych osobowych oraz sposobu ich zabezpieczenia;

4) zgłaszania ASI incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu, a także informowania ABI o przykładach naruszenia zasad ochrony danych.

§4.
Obszar przetwarzania danych osobowych

1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie jest prowadzony przez ABI – zgodnie ze wzorem stanowiącym załącznik nr 1 do Polityki Bezpieczeństwa.

2. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na

czas nieobecności w nich osób zatrudnionych, w sposób uniemożliwiający dostęp osobom trzecim. Osoby postronne mogą przebywać wewnątrz wyżej wymienionego obszaru jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych.

§5.
Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym

Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym jest prowadzony przez ABI według wzoru stanowiącego załącznik nr 2 do Polityki Bezpieczeństwa.

§6.
Struktury zbiorów danych osobowych oraz sposób przepływu danych.

1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych w zbiorach ewidencyjnych oraz poza zbiorami.
2. Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerze bazodaniowym lub stacjach roboczych.
3. Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb komórek organizacyjnych Urzędu.
4. Zawartość pól informacyjnych występujących w aplikacjach (programach) systemów zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują ADO do przetwarzania danych osobowych.
5. Na żądanie ADO lub osoby przez niego upoważnionej, kierownicy komórek organizacyjnych, w których przetwarzane są dane osobowe, zobowiązani są wskazać podstawy prawne określające zakres przetwarzanych danych.
6. Opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania między nimi wykonuje ASI na podstawie aplikacji zastosowanych do przetwarzania tych danych.
7. Opisy wykonywane są w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego ASI sporządza inne dostępne opisy struktury zbioru.
8. ASI zobowiązany jest do przekazywania opisów ABI oraz natychmiastowego informowania go o wszelkich zmianach tych opisów.
9. Schematy przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych wykonuje ASI, zgodnie z relacjami występującymi w programach służących do ich przetwarzania.
10. ASI zobowiązany jest do przekazywania schematów ABI oraz natychmiastowego informowania go o wszelkich w nich zmianach.
11. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
12. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny przy wykorzystaniu nośników zewnętrznych (np. dyskietka, CD, DVD, taśma streamera, dysk wymienny, PenDrive, itp.) lub w sposób półautomatyczny przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji (np. poprzez wewnętrzną sieć teleinformatyczną). Należy zapewnić ochronę kryptograficzną oraz zachować szczególną ostrożność podczas ich transportu i przetwarzania.

§7.
Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. ADO zapewnia zastosowanie środków technicznych, organizacyjnych i fizycznych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
2. Zastosowane środki ochrony powinny być adekwatne do poziomu ryzyka dla poszczególnych systemów, rodzaju zbiorów i kategorii danych osobowych.
3. Dokładny opis środków został zawarty w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie.
4. ABI nadzoruje i monitoruje przestrzeganie ww. środków.
5. Wymienione środki stanowią podstawę bezpieczeństwa pracy w systemie informatycznym pracowników Urzędu.
6. W przypadku zgłoszenia lub stwierdzenia zdarzenia podejrzanego, ABI przeprowadza analizę zdarzenia i dąży do wyjaśnienia przyczyny incydentu. Jeżeli incydent był celowy, ABI jest zobowiązany do pisemnego powiadomienia ADO o zdarzeniu. ADO może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych.
7. ADO udostępnia dane osobowe przetworzone we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
8. Zbiory danych udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.
9. Wniosek powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazać ich zakres i przeznaczenie.
10. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi. Podmiot ten jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych. Dane osobowe mogą być przetwarzane przez podmiot wyłącznie w zakresie, w jakim reguluje to zawarta umowa.
11. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia ustala się następujące poziomy bezpieczeństwa:
    1) podstawowy;
    2) podwyższony;
    3) wysoki;
12. Dla każdego poziomu bezpieczeństwa stosuje się odpowiednie środki bezpieczeństwa, które zostały wyszczególnione w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

WÓJT

mgr Rafał Pstrągowski

Załącznik Nr 1
do Polityki Bezpieczeństwa

WZÓR

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

Określanie obszaru, w którym przetwarzane są dane osobowe, obejmuje 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 dokumentacja papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco)

Dane osobowe przetwarzane są w budynku A, B, C Urzędu Gminy Śniadowo ul. Ostrołęcka 11; budynku Gminnego Ośrodka Kultury w Śniadowie ul. Ostrołęcka 13; budynku Biblioteki Publicznej w Śniadowie ul. Ostrołęcka 7

WYKAZ ZBIORU DANYCH OSOBOWYCH PRZETWARZANYCH W FORMIE ELEKTRONICZNEJ I/LUB W FORMIE TRADYCYJNEJ

Lp.	Nazwa zbioru danych osobowych	Pomieszczenie, w którym przetwarzane są dane osobowe	Stanowisko pracy, na którym przetwarzane są dane ze zbioru	Uwagi

Załącznik Nr 2
do Polityki Bezpieczeństwa

WZÓR

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.

Lp.	Nazwa zbioru danych osobowych	Nazwa programu (autor programu) zastosowanego do przetwarzania zbioru	Lokalizacja miejsca przetwarzania zbioru danych

Załącznik Nr 3
do Polityki Bezpieczeństwa

WZÓR

WYKAZ OSÓB, KTÓRE ZOSTAŁY ZAPOZNANE Z POLITYKĄ BEZPIECZEŃSTWA ORAZ INSTRUKCJĄ ZARZADZANIA SYSTEMEM INFORMATYCZNYM

Lp.	Imię i nazwisko	Stanowisko	Data	Podpis