ZARZĄDZENIE NR 90/2014
WÓJTA GMINY NUR

z dnia 30 grudnia 2014 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji (PBI)

Na podstawie art. 31 usatwy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2013 r., poz. 594 z późn.zm.), 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 przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.), oraz ustawy z dnia do 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2014 r., poz. 1182 z późn. zm.) zarządza się, co następuje:

§ 1. Wprowadza się Politykę Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych w Urzędzie Gminy Nur stanowiącą załącznik nr 1 oraz Instrukcję Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych stanowiącą załącznik nr 1 do Polityki Bezpieczeństwa Informacji.

§ 2. Polityka Bezpieczeństwa Informacji i Instrukcja Zarządzania Systemem Informatycznymi ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe.

§ 3. Zobowiązuje się pracowników Urzędu Gminy Nur do stosowania zasad określonych w Polityce Bezpieczeństwa Informacji.

§ 4. Tracą moc:

1) zarządzenie Nr 63/11 Wójta Gminy Nur z dnia 20 grudnia 2011 roku w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w Urzędzie Gminy w Nurze,
2) zarządzenie nr 34/2013 Wójta Gminy Nur z dnia 24 czerwca 2013 r. w sprawie zmiany zarządzenia Nr 63/11 Wójta Gminy Nur z dnia 20 grudnia 2011 roku w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w Urzędzie Gminy w Nurze,

§ 4. Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 5. Zarządzenie wchodzi w życie z dniem 1 stycznia 2015 roku.

Wójt Gminy Nur

Jacek Murawski

Załącznik nr 1 do
Zarządzenia nr 90/2014
Wójta Gminy Nur
z dnia 30 grudnia 2014r.

Polityka Bezpieczeństwa Informacji Urzędu Gminy Nur

I. Cel przygotowania polityki bezpieczeństwa informacji

Podstawowym celem przyświecającym przygotowaniu i wdrożeniu dokumentu Polityki Bezpieczeństwa było zapewnienie zgodności działania Urzędu Gminy Nur z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi. Opracowany dokument Polityki Bezpieczeństwa został w oparciu o wytyczne zawarte w następujących aktach prawnych:

1) 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. z 2004 r., Nr 100, poz. 1024 z późn. zm.),

2) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.),

3) ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (tj. Dz.U. z 2001 r. nr 128, poz. 1402 z późn. zm.).

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Polityki Bezpieczeństwa jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych. Polityka bezpieczeństwa przetwarzania danych osobowych zwana dalej „Polityką bezpieczeństwa", określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:

1) *tradycyjnych, w kartotekach, skorowidzach, aktach osobowych, wykazach, zbiorach ewidencyjnych,*
2) *w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, informacje skarbowe, ewidencje statystyczne, plany organizacyjne,*
3) *w systemach informatycznych, ewidencja mieszkańców, ewidencja małżeństw i zgonów.*

Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1) *ustawie* – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
2) *administratorze danych osobowych (ADO)* – należy przez to rozumieć Wójta Gminy Nur,
3) *administratorze sieci* – należy przez to rozumieć osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych,

4) *nośnikach danych osobowych* – należy przez to rozumieć płyty CD lub DVD, pamięci przenośne (pendrive), dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi,
5) *osobie upoważnionej (użytkownik)* – należy przez to rozumieć osobę posiadającą upoważnienie wydane przez administratora danych osobowych,
6) *danych osobowych* - należy przez to rozumieć dane osobowe zawierające wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
7) *przetwarzanie danych* - należy przez to rozumieć 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;
8) *zbiór danych* - należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów,
9) *system informatyczny* - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
10) *identyfikator użytkownika (login)* - należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
11) *hasło* - należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
12) *uwierzytelnianie* — należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
13) *poufności danych* — należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
14) *urzędzie* - należy przez to rozumieć Urząd Gminy Nur, ul. Drohiczyńskiej 2, 07-322 Nur,
15) *gminie* - należy przez to rozumieć Gminę Nur,
16) *PBI* – należy przez to rozumieć Politykę Bezpieczeństwa Informacji,

II. Postanowienia ogólne

ADO, świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności osób fizycznych powierzających urzędowi swoje dane osobowe, i do skutecznej ochrony tych danych deklaruje zamiar:

1. *Podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych, stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających.*
2. *Dane osobowe w urzędzie w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania świadomości wartości powierzonych danych osobowych jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodność urzędu.*
3. *Traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby.*
4. *Doskonalenia i rozwijania nowoczesnych metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.*

Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych urząd dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1) *przetwarzane zgodnie z prawem,*
2) *zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,*
3) *merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,*
4) *przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej jednak niż jest to niezbędne do osiągnięcia celu przetwarzania.*

W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem ADO wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności polityka bezpieczeństwa oraz instrukcje stanowiące załączniki do polityki bezpieczeństwa tj. instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych – załącznik nr 1 do PBI.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w dokumentach Polityki Bezpieczeństwa Informacji obowiązują wszystkich pracowników urzędu.

Ponadto w trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych. PBI będzie weryfikowana i dostosowywana w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji polityki bezpieczeństwa będą odbywać się nie rzadziej niż raz w roku.

III. Charakterystyka instytucji

Urząd prowadzi obsługę mieszkańców gminy, ustala i pobiera podatki rolne, od środków transportowych, od nieruchomości, zapewnia dostęp mieszkańcom do informacji dotyczącej nieruchomości, ustala i nadaje nr porządkowe działkom, prowadzi ewidencję mieszkańców, wyborców, a także ewidencjonuje i wydaje akta małżeństwa, zgonu, nadaje nr PESEL i wydaje dowody osobiste.
Obszar fizyczny przetwarzania danych obejmuje siedzibę urzędu.
Szczegółowy wykaz pomieszczeń stanowi załącznik nr 2 do niniejszej dokumentacji.

IV. Cele bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych

Pod pojęciem bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w urzędzie należy rozumieć zdolność urzędu do ochrony danych osobowych przetwarzanych w tych systemach, przed zagrożeniami, które mogą wykorzystać ich podatność i doprowadzić do udostępnienia lub ujawnienia danych osobowych nieupoważnionym podmiotom oraz zmiany lub zniszczenia danych w sposób nieautoryzowany.

Ogólnym celem prowadzonej w urzędzie polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych jest określenie poziomu bezpieczeństwa przetwarzania danych osobowych w poszczególnych systemach informatycznych eksploatowanych w urzędzie oraz określenie dla tych systemów wymagań bezpieczeństwa w zakresie środków technicznych i organizacyjnych, które powinny być odpowiednie do zagrożeń oraz kategorii danych objętych ochroną. O poufności i integralności danych osobowych

przetwarzanych w systemach informatycznych decyduje sprawność i niezawodność tych systemów oraz zabezpieczenie ich zasobów. Szczegółowe cele bezpieczeństwa wyznacza się odrębnie dla każdego systemu informatycznego, biorąc pod uwagę kategorię danych przetwarzanych w systemie i zagrożenia oraz wymagania bezpieczeństwa określone w przepisach o ochronie danych osobowych.

V. Wykaz zbiorów

1. Dane osobowe gromadzone są w zbiorach.
2. Wykaz zbiorów danych osobowych stanowi załącznik nr 3.

VI. Środki organizacyjne ochrony zbiorów danych osobowych

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

1) przetwarzanie danych osobowych w urzędzie może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań,
2) do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi załącznik nr 4 do niniejszej dokumentacji,
3) każdy pracownik podpisuje również oświadczenie zachowaniu poufności i zapoznaniu się z przepisami. Wzór oświadczenia stanowi załącznik nr 5,
4) ewidencja osób, które mają dostęp do zbiorów danych osobowych stanowi załącznik nr 6,
5) każdy pracownik urzędu musi odbyć szkolenie z zakresu ochrony danych osobowych. Za organizację szkoleń odpowiedzialny jest ADO,
6) nowo przyjęty pracownik, stażysta, uczeń będący na praktykach odbywa szkolenie z zakresu polityki bezpieczeństwa przed przystąpieniem do przetwarzania danych,
7) każdy pracownik upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi załącznik nr 7 do niniejszej dokumentacji,
8) pomieszczenia stanowiące obszar przetwarzania danych są zamykane na klucz. Każdy pracownik pobiera i zdaje klucze na sekretariacie, gdzie są one przechowywane w zamkniętej szafce,
9) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
10) przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty, pieczątki i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach,
11) obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,
12) zakazuje się pracownikom korzystania z dokumentacji służbowej, pamięci przenośnych oraz komputerów służbowych poza miejscem pracy.

VII. Odpowiedzialność za realizację polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych

Odpowiedzialność za ochronę danych osobowych w urzędzie ponoszą wszyscy pracownicy urzędu, w zakresie odpowiednim do nałożonych na nich obowiązków oraz posiadanych kompetencji.

ADO ponosi odpowiedzialność za stworzenie odpowiednich warunków prawnych, organizacyjnych i finansowych do wdrożenia systemu ochrony danych osobowych przetwarzanych w systemach informatycznych, a szczególności odpowiada za:

1) *stworzenie w urzędzie odpowiedniej struktury organizacyjnej ze stanowiskami przeznaczonymi dla osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji,*
2) *określenie kompetencji i odpowiedzialności kierowników poszczególnych komórek organizacyjnych dotyczących wykonywania zadań wynikających z przepisów o ochronie danych osobowych oraz mających związek z funkcjonowaniem systemu ochrony,*
3) *zgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych osobowych przetwarzanych w urzędzie, zgodnie z art. 41 ustawy o ochronie danych osobowych,*
4) *wprowadzenie do użytku w urzędzie:*
   a) Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych,
   b) Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Zatwierdził :

W Ó J T

Jacek Józef Murawski

.....

Administrator Danych Osobowych

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Urzędzie Gminy Nur.
2. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się środki bezpieczeństwa na poziomie wysokim.

II. Rejestrowanie w systemie informatycznym

1. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone, wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, wydane przez administratora danych osobowych.
2. Administrator Systemów Informatycznych zakłada identyfikator sieciowy/konto w systemach informatycznych i przekazuje login i hasło tymczasowe użytkownikowi. Użytkownik przy pierwszym logowaniu zobowiązany jest zmienić hasło na własne zgodnie z zasadami nadawania haseł opisanych w Rozdziale III niniejszej instrukcji.
3. Dokument nadania lub usunięcia uprawnień musi być zawsze wypełniany w przypadku zmian zakresu uprawnień.
4. Karty uprawnień są przechowywane przez Administratora Danych Osobowych.
5. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator sieci.
6. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

III. Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownik uzyskuje dostęp do danych osobowych przetwarzanych w systemie informatycznym wyłącznie po podaniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.

3. Identyfikator składa się minimalnie z 4 znaków, które nie są rozdzielone spacjami ani znakami interpunkcyjnymi. Identyfikator jest tworzony przy użyciu małych liter, z wyłączeniem polskich znaków.
4. Użytkownik, z chwilą przystąpienia do pracy w systemie informatycznym, otrzymuje hasło początkowe i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy, na swoje podając znany ciąg znaków.
5. Hasło składa się co najmniej z 8 znaków.
6. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
7. System informatyczny, który nie jest wyposażony w mechanizm wymuszający zmianę hasła po upływie 30 dni od dnia ostatniej jego zmiany, zobowiązuje użytkownika o cyklicznym co 30 dniowym zmianie tego hasła.
8. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie jego ważności.
9. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie, użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.
10. Jeśli istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie je zmienić oraz powiadomić o tym fakcie.

IV. Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu

1. Użytkownik, rozpoczynając pracę na komputerze, loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 3. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania dostępu do zbioru danych może dokonać administrator sieci w porozumieniu z administratorem danych osobowych.
4. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut następuje automatyczne włączenie wygaszacza ekranu.
5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane albo stosować blokowanie ekranu uniemożliwiające odczyt danych.
6. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.

7. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
8. Przed opuszczeniem stanowiska pracy użytkownik jest obowiązany:
   a) wylogować się z systemu informatycznego,
   b) wywołać blokowany hasłem wygaszacz ekranu.
9. Kończąc pracę użytkownik jest obowiązany:
   a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy.
10. Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się w szafach zamykanych na klucz.

V. Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu, poprzez tworzenie kopii zapasowych.
2. Za tworzenie kopii zapasowych zbiorów danych osobowych odpowiedzialny jest administrator sieci lub inna osoba przez niego wyznaczona.
3. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzanie tej procedury odpowiedzialny jest administrator sieci.
4. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
   a) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest w cykliczności comiesięcznej.
   b) kopia zapasowa danych osobowych przetwarzanych przez aplikację– pełna kopia wykonywana jest raz w tygodniu, a w przypadku wprowadzenia znacznych zmian danych osobowych, może być wykonywana częściej,
   c) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest raz do roku.
5. Kopie zapasowe przechowywane są w szafie zamykanej na klucz.

VI. Sposób, miejsce i okres przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Użytkownicy nie mogą wynosić z terenu jednostki nośników danych z zapisanymi danymi osobowymi, bez zgody administratora danych osobowych.
2. Okresowe kopie zapasowe wykonywane są na pamięciach przenośnych, płytach CD, DVD, taśmach lub innych nośnikach danych. Kopie przechowuje się w innych pomieszczeniach

niż te, w których przechowywane są zbiory danych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.

3. Dostęp do nośników z kopiami zapasowymi danych osobowych mają wyłącznie administrator danych oraz administrator sieci.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych.
5. Za zniszczenie kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiada użytkownik.
6. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 5 dni po wykorzystaniu tych danych, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania.
7. Nośniki danych podlegają komisyjnemu zniszczeniu w przypadku wycofania z eksploatacji sprzętu komputerowego, na którym przetwarzane były dane osobowe, oraz po przeniesieniu danych osobowych do zbiorów danych w systemie informatycznym z nośników, których ponowne wykorzystanie nie jest możliwe. Z przeprowadzonych czynności komisja sporządza protokół.
8. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych.

VII. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator sieci.
2. System antywirusowy zainstalowany jest w każdym komputerze z dostępem do danych osobowych. Ustawienie poziomu bezpieczeństwa i wysyłanie aktualizacji bazy sygnatur wirusów zarządzane jest centralnie.
3. Programy antywirusowe są uaktywnione przez cały czas pracy każdego komputera w systemie informatycznym.
4. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym fakcie administratora sieci.
6. Niedozwolone jest otwieranie poczty elektronicznej i od „niezaufanych" nadawców.

7. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
8. Administrator sieci jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   a) sieci lokalnej i rozległej,
   b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

VIII. Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych

1. Dane osobowe przetwarzane w jednostce mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania, na mocy ustawy o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepisy odrębne stanowią inaczej.
3. Dane udostępnione jednostce przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Administrator danych prowadzi ewidencję udostępnionych danych, która zawiera:
   a) numer ewidencyjny wydruku,
   b) zakres udostępnionych danych,
   c) adresata udostępnionych danych,
   d) datę udostępnienia.
5. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

IX. Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane przez firmy zewnętrzne pod nadzorem administratora sieci.
2. Administrator sieci okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z administratorem danych osobowych.
3. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową, co do bezpieczeństwa i stabilności nowych wersji.
4. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada administrator sieci.

5. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez administratora sieci lub firmę zewnętrzną pod nadzorem administratora sieci, a ich przyczyny analizowane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora danych osobowych.

X. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy użytkownik, który stwierdza lub podejrzewa naruszenie ochrony danych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować o tym administratora sieci.
2. Do czasu przybycia administratora sieci na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych, należy:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   d) udokumentować wstępnie zaistniałe naruszenie,
   e) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia administratora sieci.
3. Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych administrator sieci:
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania,
   b) może żądać wyjaśnień dotyczących zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   c) dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia,
   d) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia,
   e) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu administratora danych osobowych.
4. Po wyczerpaniu niezbędnych środków doraźnych, administrator sieci zasięga niezbędnych opinii i proponuje działania mające na celu usunięcie naruszenia i jego skutków oraz

ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii zapasowej i terminu wznowienia przetwarzania danych.

5. Administrator danych osobowych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który zawiera w szczególności:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób, które złożyły wyjaśnienia w związku z naruszeniem,
   b) określenie czasu i miejsca naruszenia oraz powiadomienia o naruszeniu,
   c) określenie rodzaju naruszenia i okoliczności mu towarzyszących,
   d) wyszczególnienie uwzględnionych przesłanek wyboru metody postępowania i opis podjętego działania,
   e) wstępną ocenę przyczyn wystąpienia naruszenia,
   f) ocenę przeprowadzonego postępowania wyjaśniającego i działań podjętych w celu usunięcia naruszenia i jego skutków.
6. Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, administrator sieci przeprowadza szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Zatwierdził:
WÓJT
Jacek Józef Murawski
.....
Administrator Danych Osobowych

Wykaz pomieszczeń w których odbywa się przetwarzanie danych osobowych :

Obszar, w którym są przetwarzane dane osobowe ogranicza się do budynku zlokalizowanego w Nurze przy ulicy Drohiczyńskiej 2., wymienione w poniższej tabeli oraz wszystkie w archiwum zakładowym.

L.p.	Zbiór danych osobowych	Sposób przetwarzania	Pomieszczenie
1.	Ewidencja ludności, dowody osobiste	Elektroniczny	
2.	Ewidencja przedpoborowych, poborowych i osób o nieuregulowanym obowiązku służby wojskowej	Manualny	
3.	Podatki i opłaty lokalne	Elektroniczny	
4.	Akta stanu cywilnego	Manualny	
5.	Rejestr skarg i wniosków	Manualny	
6.	Rejestr korespondencji	Manualny	
7.	Oświadczenia o stanie majątkowym pracowników urzędu	Manualny	
8.	Oświadczenia o stanie majątkowym radnych	Manualny	
9.	Ewidencja osób, którym wydano zawiadomienie o nadaniu numeru porządkowego nieruchomości	Manualny	
10.	Rejestr odbiorców wody	Elektroniczny/Manualny	
11.	Zezwolenia na sprzedaż napojów alkoholowych	Manualny	
12.	Ewidencja osób fizycznych , którym udzielono zezwolenia na wycinkę drzew i krzewów	Manualny	
13.	Ewidencja gruntów EGBV Win Gminy Nur	Elektroniczny	
14.	Akta osobowe pracowników urzędu	Manualny	
15.	Ewidencja wniosków o zmianę MPZP	Manualny	
16.	Akcyza	Manualny	
17.	Kadry	Manualny	
18.	Płace	Elektroniczny	
19.	Przelewy bankowe	Elektroniczny	
20.	Gminna Spółka Wodna	Manualny	
21.	Płatnik	Elektroniczny	
22.	Kwalifikacja wojskowa	Manualny	
23.	Księgowość zobowiązań	Elektroniczny	
24.	Gospodarka odpadami komunalnymi na terenie gminy Nur	Elektroniczny/Manualny	

Załącznik nr 3 do
Polityki Bezpieczeństwa Informacji

Wykaz zbiorów danych oraz systemów informatycznych stosowanych do przetwarzania tych zbiorów w Urzędzie Gminy Nur

L.p.	Nazwa zbioru	Rodzaj rejestru	Podlega zgłoszeniu GIODO Tak/Nie
1.	Ewidencja ludności, dowody osobiste	SELWIN,RWWIN	Nie
2.	Ewidencja przedpoborowych, poborowych i osób o nieuregulowanym obowiązku służby wojskowej	Manualny	Tak
3.	Podatki i opłaty lokalne	Podatki UINFOSYSTEM	Nie
4.	Akta stanu cywilnego	PB_USC / Manualny	Nie
5.	Rejestr skarg i wniosków	Manualny	Tak
6.	Ewidencja osób, którym wydano zawiadomienie o nadaniu numeru porządkowego nieruchomości	Manualny	Tak
7.	Rejestr odbiorców wody	WODA Bełchatów / Manualny	Tak
8.	Zezwolenia na sprzedaż napojów alkoholowych	Manualny	Nie
9.	Ewidencja osób fizycznych, którym udzielono zezwolenia na wycinkę drzew i krzewów	Manualny	Tak
10.	Ewidencja gruntów Gminy Nur	EGBV Win Geodezja	Tak
11.	Ewidencja wniosków o zmianę MPZP	Manualny	Tak
12.	Akcyza	Manualny	Tak
13.	Kadry Płace	Płace/UINFOSYSTEM/Manualny	Nie
14.	Przelewy bankowe	BS Ciechanowiec	Nie
15.	Gminna Spółka Wodna	Manualny	Nie
16.	Płatnik	Płatnik	Nie
17.	Kwalifikacja wojskowa	Manualny	Tak
18.	Księgowość zobowiązań	KSZOB/UINFOSYSTEM	Nie
19.	Ewidencja działalności gospodarczej	CEIDG	Nie
20.	System Informacji Oświatowej	SIO	Nie
21.	Podziały rozgraniczenia nieruchomości	Manualny	Tak
22.	Najem lokali	Manualny	Tak
23.	Ewidencja wniosków o wpis do CEIDG	Manualny	Tak
24.	Budowa przydomowych oczyszczalni ścieków	Manualny	Tak
25.	Gospodarka odpadami komunalnymi na terenie gminy Nur	GOMIG/ARISCO KSZOB/UINFOSYSTEM	Nie

Załącznik nr 4 do
Polityki Bezpieczeństwa Informacji

UPOWAŻNIENIE NR ..... / .....
do przetwarzania danych osobowych

Działając na podstawie uprawnień nadanych mi w Urzędzie Gminy Nur – w sprawie ochrony danych osobowych, upoważniam

Panią / Pana: ..... Do przetwarzania danych osobowych w systemach informatycznych/ nieinformatycznych funkcjonujących w Urzędzie Gminy Nur służących do przetwarzania danych osobowych .....
.....
.....
Data nadania .....
Data ustania .....

Wyżej wymieniona osoba została zapoznana z obecnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w obowiązkach służbowych i zgodnie z Ustawą z dnia 29.08.1997 r. o ochronie danych osobowych (t. j. Dz. U z 2014r, poz.1182 z późn. zm.) i wydanych do niej przepisach wykonawczych oraz w Zarządzeniu Nr 10/2015 Wójta Gminy Nur z dnia 30 stycznia 2015 r., w sprawie ochrony danych osobowych.
Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Gminy Nur.

.....
Podpis osoby wystawiającej upoważnienie

.....
Data i czytelny podpis osoby upoważnionej

Załącznik nr 5 do
Polityki Bezpieczeństwa Informacji

OŚWIADCZENIE

o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany(a) ..... oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:

a) zadań i obowiązków służbowych wynikających z umowy o pracę,
b) zadań wynikających z umowy cywilno-prawnej,
c) zadań wynikających z umowy - w związku z praktyką studencką,
d) porozumieniem dotyczącym odbycia stażu,

zarówno w trakcie wykonywania umowy, jak i po jej ustaniu :

Zobowiązuję się przestrzegać polityki, instrukcji i procedur, obowiązujących w Urzędzie Gminy Nur. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów znajdujących się w Urzędzie Gminy Nur. Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Urzędzie Gminy Nur zasadach, dotyczących przetwarzania danych osobowych, określonych w „Polityce Bezpieczeństwa Informacji".

Oświadczam, że zostałem(am) zapoznany(a) z przepisami ustawy o ochronie danych osobowych (Dz. U. z 2014 r., poz.1182 z późn. zm.) 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 (Dz. U. Nr 100, poz. 1024 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów rozdziału 8 ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w Urzędzie Gminy Nur może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....
(Miejscowość i data)

.....
(Czytelny podpis osoby składającej oświadczenie)

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH

LP.	*Imię i Nazwisko osoby upoważnionej*	*Data nadania upoważnienia*	*Data ustania upoważnienia*	*Zakres upoważnienia*	*Identyfikator w systemie informatycznym*
1.					
2.					
3.					
4.					
5.					

Załącznik nr 7 do
Polityki Bezpieczeństwa Informacji

.....
Miejscowość i data

OŚWIADCZENIE PRACOWNIKA O ZAPOZNANIU SIĘ Z TREŚCIĄ POLITYKI BEZPIECZEŃSTWA INFORMACJI

Niżej podpisany/a ....., zam. w .....Zatrudniony/a w (zakładzie pracy) .....

Na stanowisku.....

potwierdzam, że zostałem/am, zapoznany/a z Polityką Bezpieczeństwa Informacji Urzędu Gminy Nur , co potwierdzam własnoręcznym podpisem.

.....
Czytelny podpis pracownika