Zarządzenie Nr 0050.358.2016
Wójta Gminy Nędza
z dnia 19.10.2016 r.

w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r. poz. 922) oraz § 3 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. z 2004 r. Nr 100 poz. 1024).

zarządzam, co następuje:

§ 1

1. Wprowadza się w Urzędzie Gminy Nędza szczegółowe zasady ochrony danych osobowych, opisane w załącznikach do niniejszego zarządzenia.
2. Wszystkich pracowników Urzędu Gminy, a w szczególności przetwarzających dane osobowe, zobowiązuje się do zapoznania z niniejszym zarządzeniem wraz z załącznikami i do przestrzegania zawartych w nim zasad.

§2

Wprowadzam do stosowania w Urzędzie Gminy:
1. Politykę Bezpieczeństwa, która stanowi załącznik nr 1 do niniejszego zarządzenia.
2. Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, który stanowi załącznik nr 2 do niniejszego zarządzenia.
3. Upoważnienia do przetwarzania danych osobowych, który stanowi załącznik nr 3 do niniejszego zarządzenia.
4. Oświadczenie , które stanowi załącznik nr 4 do niniejszego zarządzenia.

§3

Traci moc Zarządzenie Nr 0050.172.2015 Wójta Gminy Nędza z dnia 01 czerwca 2015 roku w sprawie: wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§4

Zarządzenie wchodzi w życie z dniem podjęcia.

Załącznik nr 1
do Zarządzenia nr 0050.358.2016
Wójta Gminy Nędza
z dnia 19.10.2016 r.

POLITYKA BEZPIECZEŃSTWA

I. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Dane osobowe przetwarzane są w budynku UG Nędza, ul. Jana III Sobieskiego 5.

Lp.	Nazwa zbiorów danych osobowych	Pomieszczenia w których przetwarzane są zbiory danych osobowych	Stanowisko przetwarzające zbiory danych osobowych
1	Urząd Stanu Cywilnego	Pok. Nr 1	Kierownik Urzędu Stanu Cywilnego
2	Ewidencja ludności i dowodów osobistych	Pok. Nr 3	Inspektor ds. Ewidencji Ludności, Dowodów Osobistych, Ewidencji Działalności Gospodarczej
3	Ewidencja płatników i dłużników podatków i opłat Gminy Nędza	Pok. Nr 5	Inspektor ds. Księgowości Podatkowej
4	Rejestr podatków Gminy Nędza	Pok. Nr 5	Inspektor ds. Wymiaru Podatków i Opłat
5	Kwalifikacja wojskowa- rejestr	Pok. Nr 7	Podinspektor ds. Informatyki i Ochrony
6	System informacji oświatowej	Pok. Nr 9	Główny Specjalista ds. Oświaty i Sportu
7	Dzierżawa gruntów i opłaty za wieczyste użytkowanie gruntów	Pok. Nr 10	Specjalista ds. Gospodarki Gruntami i Geodezji
8	Plany obronne gminy, obrony cywilnej gminy, zarządzania kryzysowego gminy	Pok. nr 11	Główny Specjalista ds. Obronnych i Reagowania Kryzysowego
9	Oświadczenia majątkowe radnych	Pok. Nr 3	Sekretarz
10	Ewidencja najemców mieszkaniowego zasobu gminy	Pok. Nr 14	Specjalista ds. Rolnictwa i Gospodarki Zasobami Gminy
11	Ewidencja egzekucji administracyjnej w zakresie opłaty za gospodarowanie odpadami komunalnymi	Pok. Nr 2	Podinspektor ds. Wymiaru Opłaty Za Gospodarowanie Odpadami Komunalnymi
12	Ewidencja gospodarki odpadami komunalnymi	Pok. Nr 2	Podinspektor ds. Wymiaru Opłaty Za Gospodarowanie Odpadami Komunalnymi
13	Rejestr- wycinka drzew	Pok. Nr 23	Referent ds. Zagospodarowania Przestrzennego
14	Rejestr- zawiadomienie stron o przeznaczeniu terenu, postanowienia wstępne projektu podziału nieruchomości, renty planistyczne	Pok. Nr 23	Referent ds. Zagospodarowania Przestrzennego
15	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu	Pok. Nr 23	Referent ds. Zagospodarowania Przestrzennego

II. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

Lp.	Nazwa zbiorów danych osobowych	Programy zastosowane do przetwarzania danych	Stanowisko przetwarzające zbiory danych osobowych
1	Urząd Stanu Cywilnego	Program PB-USC Komputerowy System Rejestracji	Kierownik Urzędu Stanu Cywilnego
2	Ewidencja ludności i dowodów osobistych	Program System Wydawania Dowodów Osobistych	Inspektor ds. Ewidencji Ludności, Dowodów Osobistych, Ewidencji Działalności Gospodarczej
3	Ewidencja płatników i dłużników podatków i opłat Gminy Nędza	Program Podatki i Opłaty Gminne	Inspektor ds. Księgowości Podatkowej
4	Rejestr podatków Gminy Nędza	Program Podatki i Opłaty Gminne	Inspektor ds. Wymiaru Podatków i Opłat
5	Kwalifikacja wojskowa- rejestr	Ewidencja papierowa	Podinspektor ds. Informatyki i Ochrony
6	System informacji oświatowej	Program SIO	Główny Specjalista ds. Oświaty i Sportu
7	Dzierżawa gruntów i opłaty za wieczyste użytkowanie gruntów	Ewidencja papierowa	Specjalista ds. Gospodarki Gruntami i Geodezji
8	Plany obronne gminy, obrony cywilnej gminy, zarządzania kryzysowego gminy	Ewidencja papierowa	Główny Specjalista ds. Obronnych i Reagowania Kryzysowego
9	Oświadczenia majątkowe radnych	Ewidencja papierowa	Sekretarz
10	Ewidencja najemców mieszkaniowego zasobu gminy	Ewidencja papierowa	Specjalista ds. Rolnictwa i Gospodarki Zasobami Gminy
11	Ewidencja egzekucji administracyjnej w zakresie opłaty za gospodarowanie odpadami komunalnymi	Program Podatki i Opłaty Gminne	Podinspektor ds. Wymiaru Opłaty Za Gospodarowanie Odpadami Komunalnymi
12	Ewidencja gospodarki odpadami komunalnymi	Program Podatki i Opłaty Gminne	Podinspektor ds. Wymiaru Opłaty Za Gospodarowanie Odpadami Komunalnymi
13	Rejestr- wycinka drzew	Ewidencja papierowa	Referent ds. Zagospodarowania Przestrzennego
14	Rejestr- zawiadomienie stron o przeznaczeniu terenu, postanowienia wstępne projektu podziału nieruchomości, renty planistyczne	Ewidencja papierowa	Referent ds. Zagospodarowania Przestrzennego
15	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu	Ewidencja papierowa	Referent ds. Zagospodarowania Przestrzennego

III. Opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi:

1. Zbiór danych „ Urząd Stanu Cywilnego w Nędzy” zawiera następujące pola:

- Nazwiska i imiona
- Imiona rodziców
- Data urodzenia
- Adres zamieszkania lub pobytu
- Nr PESEL
- Zawód
- Wykształcenie
- Seria i nr dowodu osobistego
- Kolor oczu
- Wzrost w cm

- Płeć
- Kod pocztowy
- Przyczyna wystawienia dowodu
- Podpis osoby
- Fotografia

2. Zbiór danych „ Ewidencja ludności i dowodów osobistych” zawiera następujące pola:

- Imiona i nazwiska
- Imiona i nazwiska rodowe rodziców
- Nazwisko rodowe
- Data urodzenia
- Miejsce urodzenia
- Numer PESEL
- Kolor oczu
- Wzrost w cm
- Płeć
- Adres zamieszkania
- Rodzaj zameldowania
- Kod pocztowy
- Posiadany dotychczasowy dokument tożsamości (seria, nr, nazwa i siedziba wystawcy)
- Przyczyna wystawienia dowodu
- Data i przyczyna utraty
- Podpis osoby
- Fotografia
- Dane osobowe/ nazwiska i imiona, nazwisko rodowe i z poprzedniego małżeństwa, imiona rodziców, data urodzenia, miejsce urodzenia, akta urodzenia, data i nr USC
- Dane osobowe archiwalne/nazwiska i imiona, nazwisko rodowe i z poprzedniego małżeństwa
- Adres zamieszkania lub pobytu stałego oraz data zameldowania
- Adres czasowy oraz czas pobytu czasowego
- Archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania
- Dokument tożsamości/ rodzaj dokumentu, seria i numer dowodu, wystawca dokumentu, rysopis: wzrost, kolor oczu, znaki szczególne
- Numer ewidencyjny PESEL
- USC i nr aktu urodzenia
- Stan cywilny/ imię i nazwisko współ małżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa, data zawarcia małżeństwa, USC i numer aktu małżeństwa, data wydania i wydający dokument tożsamości
- Stan cywilny archiwalny/ imię i nazwisko współmałżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa, data zawarcia małżeństwa, USC i numer aktu małżeństwa
- Data wydania i wydający dokument tożsamości
- Archiwalne dokumenty tożsamości
- Obowiązek wojskowy/czy podlega obowiązkowi, nazwa i nr wojskowego dokumentu tożsamości, stopień wojskowy
- Data zgonu, USC i numer aktu zgonu
- Imiona i nazwiska rodowe
- Narodowość
- Obywatelstwo (data zmiany, podstawa prawna)
- Adnotacje o rozwodzie

3. **Zbiór danych „ Ewidencja płatników i dłużników podatków i opłat Gminy Nędza” zawiera następujące pola:**
    - Nazwiska i imiona
    - Imiona rodziców
    - Data urodzenia
    - Adres zamieszkania lub pobytu
    - Nr PESEL
    - Miejsce pracy

4. **Zbiór danych „ Rejestr podatków Gminy Nędza” zawiera następujące pola:**
    - Nazwiska i imiona
    - Imiona rodziców
    - Data urodzenia
    - Adres zamieszkania lub pobytu
    - Nr PESEL
    - Miejsce pracy

5. **Zbiór danych „ Kwalifikacja wojskowa- rejestr” zawiera następujące pola:**
    - Nazwiska i imiona
    - Imiona rodziców
    - Data urodzenia
    - Adres zamieszkania lub pobytu
    - Nr PESEL
    - Seria i nr dowodu osobistego
    - Nazwisko rodowe przedpoborowych

6. **Zbiór danych „ System informacji oświatowej” zawiera następujące pola:**
    - Data urodzenia
    - Nr PESEL
    - Wykształcenie
    - Płeć
    - Formy i wymiar zatrudnienia
    - Stopień awansu zawodowego
    - Przygotowanie pedagogiczne
    - Formy kształcenia i doskonalenia
    - Sprawowane funkcje i zajmowane stanowiska
    - Rodzaj prowadzonych zajęć albo przyczyny nieprowadzenia zajęć
    - Staż pracy
    - Wysokość wynagrodzenia, z wyszczególnieniem jego składników
    - Wysokość dodatków

7. **Zbiór danych „ Dzierżawa gruntów i opłaty za wieczyste użytkowanie gruntów” zawiera następujące pola:**
    - Nazwiska i imiona
    - Adres zamieszkania lub pobytu

8. **Zbiór danych „ Plany obronne gminy, obrony cywilnej gminy, zarządzania kryzysowego gminy” zawiera następujące pola:**
    - Nazwiska i imiona
    - Imiona rodziców
    - Data urodzenia
    - Miejsce urodzenia
    - Adres zamieszkania
    - Nr telefonu

9. **Zbiór danych „ Oświadczenia majątkowe radnych” zawiera następujące pola:**
    - Imiona nazwiska
    - Adres zamieszkania lub pobytu
    - Miejsce pracy
    - Seria i nr dowodu osobistego
    - Informacje o stanie majątkowym
    - Informacje o prowadzonej działalności gospodarczej

10. **Zbiór danych „ Ewidencja najemców mieszkaniowego zasobu gminy” zawiera następujące pola:**
    - Nazwiska i imiona
    - Adres zamieszkania lub pobytu

11. **Zbiór danych „ Ewidencja egzekucji administracyjnej w zakresie opłaty za gospodarowanie odpadami komunalnymi” zawiera następujące pola:**
    - Nazwiska i imiona
    - Imiona rodziców
    - Data urodzenia
    - Miejsce urodzenia
    - Adres zamieszkania lub pobytu
    - Numer ewidencyjny PESEL
    - Miejsce pracy
    - Seria i numer dowodu osobistego
    - Numer telefonu

12. **Zbiór danych „ Ewidencja gospodarki odpadami komunalnymi” zawiera następujące pola:**
    - Nazwiska i imiona
    - Imiona rodziców
    - Data urodzenia
    - Adres zamieszkania lub pobytu
    - Numer ewidencyjny PESEL
    - Numer Identyfikacji Podatkowej

13. **Zbiór danych „ Rejestr wycinka drzew” zawiera następujące pola:**
    - Nazwiska i imiona
    - Adres zamieszkania lub pobytu
    - Lokalizacja drzew przeznaczonych do wycinki
    - Nazwiska i imiona członków komisji

14. **Zbiór danych „ Rejestr- zawiadomienie stron o przeznaczeniu terenu, postanowienia wstępne projektu podziału nieruchomości, renty planistyczne” zawiera następujące pola:**
    - Nazwiska i imiona
    - Adres Zamieszkania lub pobytu
    - Nr telefonu

15. **Zbiór danych „ Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu” zawiera następujące pola:**
    - Nazwiska i imiona
    - Adres zamieszkania lub pobytu
    - Rodzaj, charakterystyka i lokalizacja zamierzonej inwestycji

IV. Sposób przepływu danych pomiędzy poszczególnymi systemami

- Brak przepływu danych pomiędzy poszczególnymi systemami

V. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Środki ochrony fizycznej:

- Budynek Urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest zamykany po zakończeniu pracy oraz zabezpieczany alarmem.
- Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonymi zamkami patentowymi.
- Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej w Urzędzie Gminy Nędza lub w obecności Wójta Gminy.
- Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności w nich osób zatrudnionych w Urzędzie Gminy Nędza, w sposób uniemożliwiający dostęp do nich osób trzecich.
- 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.
- Do przebywania w pomieszczeniu serwera uprawnieni są: Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego, osoby odpowiedzialne za obsługę informatyczną urzędu oraz kierownik urzędu.
- Przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. 6, a w przypadku ich nieobecności- w obecności osoby pisemnie upoważnionej przez kierownika urzędu.

2. Środki sprzętowe, informatyczne i telekomunikacyjne:

- Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki dokumentów).
- Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej centralnym UPS- em.
- Przeznaczono komputer w celu archiwizacji danych z poszczególnych komputerów użytkowych.
- Na wszystkich serwerach oraz stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym przed przesłaniem jej do Użytkowania.
- Archiwizacje wykonywane są na płytach CD, oraz na odrębnym komputerze zabezpieczone hasłem w zamykanym pomieszczeniu.

3. Środki ochrony w ramach oprogramowania systemu:

- Dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla osób zajmujących się obsługą informatyczną Urzędu.
- Konfiguracja systemu umożliwia Użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
- System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
- W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do sieci.

4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

- Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji, chyba że program tego nie przewiduje wówczas jedynym środkiem zabezpieczającym jest hasło systemowe.
- Dla każdego Użytkownika systemu jest ustalony odrębny identyfikator.
- Zdefiniowano Użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

5. Środki ochrony w ramach systemu użytkowego:

- Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności Użytkownika.
- Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

6. Środki organizacyjne:

- Administrator Danych Osobowych przyznaje uprawnienia w zakresie dostępu do systemu informatycznego określającego zakres uprawnień pracownika.
- Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
- Wprowadzono instrukcję zarządzania systemem informatycznym.

Załącznik nr 2
do Zarządzenia nr 0050.358.2016
Wójta Gminy Nędza
z dnia 19.10.2016 r.

……
Nazwa jednostki organizacyjnej

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Administrator danych:
   - Nadaje upoważnienie w zakresie dostępu do systemu informatycznego osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych w systemie;
   - Przekazuje wypełniony dokument w postaci papierowej:
     - 1 egz. do kadr- celem umieszczenia w teczce akt osobowych,
     - 1 egz. do osoby której upoważnienie dotyczy,
     - 1 egz. do Administrator Bezpieczeństwa Informacyjnego (ABI).

2. ABI:
   - Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
     a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
     b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
     c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   - Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
   - Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób.
   - Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisywane są dane osobowe.
   - Nadzór nad zarządzaniem hasłami użytkowników i przestrzeganiem procedur określających częstotliwość ich zmiany.
   - Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych.
   - Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
   - Kontrola nad danymi osobowymi wprowadzonymi do zbiorów (przez kogo zostały wprowadzone, komu są przekazywane).
   - Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń.
   - Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe.
   - Nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych.
   - Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.

3. ASI:

- Formułowanie, w uzgodnieniu z administratorem danych i/lub osobami, do których administrator delegował zarządzanie uprawnieniami oraz ABI, sposobu określania uprawnień w systemach informatycznych.
- Realizacja decyzji Administratora Danych Osobowych (innych) odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT Urzędu tj.:

a) tworzenie kont użytkowników w systemach informatycznych,
b) przypisywanie, do kont, startowych haseł uwierzytelniających użytkowników tych kont,
c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
d) resetowanie utraconych haseł,
e) usuwanie kont i uprawnień dla kont osób które zakończyły pracę w Urzędzie,
f) dostarczanie ABI informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych.

- Planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie Gminy.
- Planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych.
- Automatyzacja zadań konserwacyjnych w systemie – w tym wykonywania kopii zapasowych oprogramowania i danych.
- Monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników.
- Monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych.
- Zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych.
- Systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego.
- Zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki.
- Rozwiązywanie, samodzielnie i we współpracy z pozostałym personelem IT, problemów towarzyszących eksploatacji systemów informatycznych.
- Przygotowywanie, we współpracy z ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji.
- Prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT.

4. Użytkownik:
    - Uwierzytelnia się w systemie po podaniu identyfikatora oraz hasła uzyskanego od Informatyka;
    - Użytkownik zmienia hasło na swoje, którego nie przekazuje nikomu i może rozpocząć pracę w aplikacji.

5. Użytkownik jest wyrejestrowany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień dostępu do danych osobowych, co ma miejsce w przypadku:
    - Ustania zatrudnienia;
    - Zmiany zakresu obowiązków;
    - Utraty uprawnienia.

6. Informację pisemną o ustaniu zatrudnienia, zmianie zakresu obowiązków i utracie upoważnienia, przekazują kadry do ABI z chwilą ich zaistnienia.

II. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzeniem i użytkowaniem

1. W systemie informatycznym stosuje się uwierzytelnienia dwustopniowe; na poziomie:
    - Dostępu do sieci lokalnej;
    - Dostępu do aplikacji.

2. Do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła.

3. Hasło dostępu do sieci lokalnej składa się, co najmniej z 4 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.

5. Hasło nie może być ujawnione nawet po utracie przez nie ważności.

6. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

7. Dla każdej osoby upoważnionej instalowany jest odrębny identyfikator i hasło, tak, aby bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym mogła mieć tylko ta osoba, która poda właściwy identyfikator i hasło.

8. Identyfikator użytkownika jest wpisywany do ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym wraz z zakresem upoważnienia oraz datą nadania uprawnień.

9. Aplikacja wymusi na użytkowniku zmianę hasła, co 30 dni.

10. System zostanie wyłączony po trzykrotnej próbie nieudanego logowania się.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Rozpoczęcie pracy:
    - Uruchomienie komputera w systemie podając hasło;
    - Uruchomienie komputera i zalogowanie się podając swój identyfikator dostępu do sieci;
    - Uruchomienie aplikacji, wpisując swój identyfikator i hasło dostępu- uzależnione od programu;

- Rozpocząć pracę.

2. Procedura zawieszenia pracy w systemie:
   - Przy każdym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlone dane osobowe
   - Przed opuszczeniem miejsca pracy na dłuższy czas użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz ekranu

3. Procedura zakończenia pracy w systemie:
   - Zarchiwizować dane
   - Zamknąć aplikację
   - Zamknąć system
   - Wyłączyć monitor i drukarkę

IV. Procedury tworzenia kopii zapasowych i zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. W cyklu dziennym kopie wykonywane są w serwerze oraz na odrębnym stanowisku komputerowym pełniącym funkcję archiwum.
2. W razie potrzeby kopie zapasowe wykonywane są przez użytkowników aplikacji na płytach lub dyskietkach.
3. Informatyk sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

V. Sposób, miejsce i okres przechowywania:

1. Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich przez osoby nieupoważnione.
2. Wydruki, zawierające dane osobowe , należy zniszczyć przez pocięcie w niszczarce nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
3. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
4. Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych lub szafach pancernych
5. Przeznaczone do likwidacji elektroniczne i optyczne nośniki informacji, mogące zawierać dane osobowe, pozbawia się w sposób trwały zapisu tych danych, a w przypadku gdy nie jest to możliwe, niszczy lub uszkadza się w sposób trwale uniemożliwiający ich odczytanie, nie później niż po upływie 3 dni.
6. Za skasowanie zbędnych danych lub zniszczenie zbędnych nośników elektronicznych odpowiedzialny jest Administrator Systemu Informatycznego.
7. Kopie zapasowe zbioru danych osobowych przechowywane są w serwerowni.
8. Dostęp do serwerowni mają tylko upoważnieni pracownicy, tj. ABI i Informatyk.
9. Kopie zapasowe przechowuje się przez okres:
   - dzienne -przez siedem dni;
   - tygodniowe -do końca następnego tygodnia;
   - miesięczne -dwunastu miesięcy następujących po miesiącu sporządzenia kopii, dopuszcza się dłuższy okres przechowywania, o ile pozwalają na to warunki;
   - roczne -nieograniczony.
10. Dane osobowe zapisane w formie papierowej inne niż wydruki z systemu (pisma, ankiety itp.) są przechowywane na podobnych zasadach, co wydruki.
11. W przypadku konieczności przekazywania elektronicznych lub optycznych nośników informacji zawierających dane osobowe podmiotom zewnętrznym w sytuacjach nie związanych z wykonywanymi działaniami służbowymi, nośniki te pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.

VI. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego lub inna ingerencja w ten system.

1. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Informatyk.
2. Oprogramowanie zastosowane w systemach informatycznych automatycznie monitoruje występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji.
3. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje Informatyk, wykorzystując w trakcie pracy moduł programu antywirusowego z aktualną bazą antywirusową.
5. Administrator Systemu Informatycznego ma obowiązek zgłaszać na piśmie Administratorowi Danych Osobowych wszelkie potrzeby lub zauważone niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego.
6. O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ABI lub Informatyka
7. W przypadku, gdy system zabezpieczeń wskazuje zaistnienie zagrożenia, użytkownicy są zobowiązani bezzwłocznie powiadomić o tym fakcie Informatyka, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności.
8. Informatyk jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
    - Sieci lokalnej;
    - Stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
9. Ochrona systemu informatycznego używanego w urzędzie polega na:
    - Ochronie przez identyfikatora;
    - Ochronie za pomocą hasła;
    - Przydzielaniu praw;
    - Nadawaniu atrybutów.
10. Bezwzględnie zakazuje się użytkownikom samowolnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji (magnetycznych, optycznych, urządzeń podłączanych do stacji roboczych). Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody Informatyka, po uprzednim sprawdzeniu nośnika informacji przez Informatyka pod względem bezpieczeństwa dla systemu informatycznego.
11. Bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić Administratora Bezpieczeństwa Informacji oraz Informatyka.

VII. Zasady i sposób odnotowania w systemie informacji o udostępnianiu danych osobowych.

1. W komórce organizacyjnej w której przetwarzane są dane osobowe prowadzi się rejestr. W niektórych aplikacjach możliwe jest odnotowanie informacji o odbiorcach danych z tego systemu.
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
    - Osoby, której dane dotyczą;
    - Osoby użytkowania systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w urzędzie;
    - Przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych;
    - Podmiotu, któremu powierzono przetwarzanie danych;
    - Organów państwowych lub organów samorządu terytorialnego, któremu dane są udostępnione w związku z prowadzonym postępowaniem.
3. Odnotowanie obejmuje informacje o:

- Nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane;
- Zakresie udostępniania danych;
- Dacie udostępniania.

4. Udostępnianie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych.
5. Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje ABI.

VIII. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. O przeprowadzonych przeglądach i konserwacjach systemu każdorazowo informowany jest ABI, który może nadzorować przebieg prac.
2. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji dokonuje stosownie do potrzeb Informatyk w porozumieniu z ABI.
3. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada Informatyk.
4. Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
5. Użytkownik ma obowiązek niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub Informatyka o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
6. Sprawdzanie poprawności działania programów i narzędzi programowych przeprowadza się w następujących przypadkach
    - Zmiany wersji oprogramowania serwera plików;
    - Zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu;
    - Zmiany systemu operacyjnego serwera plików;
    - Zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu;
    - Wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
7. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzanie powinno obejmować:
    - Poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika);
    - Poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty).
8. Poprawność funkcjonowania aplikacji polega na symulacji działania wykonujące następujące operacje:
    - Wprowadzania danych osobowych;
    - Edytowania danych osobowych;
    - Wyszukiwania danych osobowych;
    - Wydruku danych osobowych.
9. Przegląd przeprowadza projektant nowego systemu w obecności Informatyka.
10. Za prawidłowość przeprowadzania przeglądów i konserwacji systemu odpowiada Informatyk.
11. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
12. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania.

Załącznik nr 3
do Zarządzenia nr 0050.358.2016
Wójta Gminy Nędza
z dnia 19.10.2016 r.

Zbiór danych osobowych o nazwie:

Upoważnienie do przetwarzania danych osobowych Nr

Na podstawie art. 37 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2016 r. poz. 922) oraz §4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024)

Upoważniam Panią/Pana……..……..
Zatrudnioną/ zatrudnionego na stanowisku……..

do dostępu do następujących danych osobowych:

– …….
–…….

Ustalam Panu/ Pani Następujący zakres odpowiedzialności za ochronę zbioru danych j.w. przed nieupoważnionym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem:

1. Zobowiązuję Pana/Panią do przestrzegania postanowień Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych;
2. Zobowiązuję Pana/Panią do stosowania przepisów ustawy przy przetwarzaniu danych osobowych w:
   - Systemie informatycznym;
   - Kartotekach;
   - Skorowidzach;
   - Księgach;
   - Wykazach i innych zbiorach ewidencyjnych.
3. Zobowiązuję Pana/Panią do zachowania w tajemnicy danych osobowych w czasie zatrudnienia po ustaniu zatrudnienia.

W ramach wykonywanych czynności służbowych

Podpis Administratora Danych Osobowych Podpis Pracownika

Zobowiązanie pracownika
Zobowiązuje się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), również po ustaniu stosunku pracy, oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych.

Podpis Pracownika

Załącznik nr 4
do Zarządzenia nr 0050.358.2016
Wójta Gminy Nędza
z dnia 19.10.2016 r.

.....
Imię i nazwisko

.....
Stanowisko pracy

.....
Nazwa zbioru danych osobowych

OŚWIADCZENIE

Niniejszym oświadczam, że zapoznałem się z:

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz 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).
- Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

I zobowiązuję się do ich przestrzegania.

.....
Podpis pracownika

UMOWA POWIERZENIA
Nr 1/2011

zawarta w dniu …….
pomiędzy :

Gminą Nędza w imieniu której działa

Wójt Gminy Nędza Anna Iskała

zwaną w dalszej części **„ADMINISTRATOR DANYCH OSOBOWYCH”**

a

……

……

reprezentowanym przez …….

zwanym w dalszej części **„PODMIOTEM”**

§ 1

Przedmiot umowy

1. Strony niniejszą umowę zawierają w trybie art. 31 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)
2. Administrator Danych Osobowych powierza Podmiotowi w drodze niniejszej umowy przetwarzanie danych osobowych w zakresie zbioru pn. …….. celem ……..

§ 2

Zakres przetwarzanych danych osobowych

Przetwarzanie danych jest dopuszczalne tylko w zakresie:

§ 3

Obowiązki Podmiotu

1. Podmiot może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.
2. Podmiot jest obowiązany podjąć środki zabezpieczające zbiór danych zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)
3. Podmiot w przypadku kontroli zgodności przetwarzania danych przez Generalnego Inspektora Ochrony Danych Osobowych zobowiązuje się do stosowania odpowiednio przepisów art. 14-19 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. z późn. zm.
4. Podmiot powinien dołożyć szczególnej staranności w celu ochrony interesu osób, których dane dotyczą zgodnie z art. 26- 27 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
5. Podmiot zobowiązuje się do przestrzegania przepisów zawartych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
6. Podmiot zobowiązuje się do informowania Administratora Danych Osobowych o zmianach w §2 niniejszej umowy tj. zakres przetwarzanych danych.
7. Osoba do kontaktów roboczych

§ 4

Obowiązki Administratora Danych Osobowych

1. Administrator jest zobowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zgodnie z art. 41 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
2. Administrator jest zobowiązany do wprowadzenia niniejszego zbioru u do Polityki Bezpieczeństwa Informacji Gminy Nędza
3. Administrator jest zobowiązany do zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.
4. Administrator zobowiązuje się do aktualizacji Polityki Bezpieczeństwa na podstawie informacji Podmiotu

§ 5

Odpowiedzialność stron

Odpowiedzialność za przestrzeganie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych spoczywa na Administratorze Danych osobowych oraz Podmiocie.

§ 6

W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

§ 7

Wszelkie zmiany w niniejszej umowie mogą nastąpić jedynie w formie pisemnej.

§ 8

Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Administrator Danych Osobowych: **Podmiot:**

....