Zarządzenie nr 22/2016
Wójta gminy Naruszewo
z dnia 5 kwietnia 2016 roku
w sprawie ochrony danych osobowych w Urzędzie Gminy w Naruszewie

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 ze zm.), § 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. Nr 100, poz. 1024) oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2013 r. poz. 594 ze zm.) zarządza się, co następuje:

§1.

W Urzędzie Gminy w Naruszewie wprowadza się:

1) politykę bezpieczeństwa, stanowiącą załącznik nr 1 do zarządzenia;
2) instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do zarządzenia.

§2.

Zobowiązuje się wszystkich pracowników Urzędu Gminy w Naruszewie do zapoznania się z niniejszym zarządzeniem i załącznikami do zarządzenia w terminie do 30 kwietnia 2016 roku oraz do przestrzegania zasad zawartych w tych dokumentach. Oświadczenie o zapoznaniu się należy wpiąć do akt osobowych pracowników Urzędu Gminy w Naruszewie.

§3.

Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy.

§4.

Traci moc Zarządzenie nr 35/09 Wójta Gminy Naruszewo z dnia 4 sierpnia 2009 roku **w** sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych.

§5.

Zarządzenie wchodzi w życie od 1 maja 2016 roku.

Wójt
mgr inż. Beata Pierścińska

Załączniki nr 1
do zarządzenia nr 22/2016
Wójta Gminy Naruszewo
z dnia 5 kwietnia 2016 roku

POLITYKA BEZPIECZEŃSTWA W URZĘDZIE GMINY W NARUSZEWIE

Rozdział I
Postanowienia ogólne, definicje

§1.

1. Polityka Bezpieczeństwa w Urzędzie Gminy w Naruszewie jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Urząd Gminy w Naruszewie.
2. Podstawą do opracowania i wdrożenia dokumentu są:
   1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 ze zm.);
   2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 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).
3. Przetwarzanie danych osobowych w Urzędzie Gminy w Naruszewie jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych w tym niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które powinny być spójne z polityką bezpieczeństwa informacji wymaganą przez ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne.
4. Polityka Bezpieczeństwa ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Urzędzie Gminy w Naruszewie, w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

§2.

Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:

1) OchrDanychU – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 poz. 2135 ze zm.);
2) Rozporządzenie – 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. Nr 100, poz. 1024);
3) Urząd – Urząd Gminy w Naruszewie;
4) Administrator Danych Osobowych – Wójta Gminy w Naruszewie zwanego dalej „ADO";

5) Administrator Bezpieczeństwa Informacji – osobę powołaną przez Wójta Gminy w Naruszewie, wpisaną do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych rejestru administratorów bezpieczeństwa informacji, zwaną dalej „ABI";
6) Administrator Systemów Informatycznych – osobę wyznaczoną przez Wójta Gminy w Naruszewie, zwaną dalej „ASI";
7) Lokalnym Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć Kierownika Referatu lub pracownika zatrudnionego na samodzielnym stanowisku, przewidzianych w strukturze organizacyjnej Urzędu;
8) użytkowniku danych osobowych – należy przez to rozumieć każdego pracownika, który wykonując czynności służbowe przetwarza dane osobowe, tzn. wykonuje na nich jakiekolwiek operacje, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie.

Rozdział II
Obszary przetwarzania danych osobowych

§3.

1. Obszar przetwarzania danych osobowych w Urzędzie obejmuje budynek Urzędu, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje), oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).
2. Obszar przetwarzania danych osobowych określony jest w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe", stanowiącym załącznik nr 1 do Polityki Bezpieczeństwa Informacji. Wykaz ten zawiera następujące informacje:
   1) lokalizację budynku,
   2) numer pomieszczenia i jego przeznaczenie,
   3) wskazanie piętra budynku,
   4) określenie referatu użytkującego dane pomieszczenie,
   5) wskazanie liczby osób pracujących w pomieszczeniu: wskazanie stanowisk i liczby osób,
   6) określenie zabezpieczenia pomieszczenia.
3. Obszar przetwarzania danych oraz warunki ochrony tego obszaru określone zostały w załączniku nr 2 do Polityki Bezpieczeństwa Informacji „Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe".

§4.

Wykaz zbiorów danych przetwarzanych w Urzędzie Gminy określony został w załączniku nr 3 do Polityki Bezpieczeństwa Informacji – „Wykaz zasobów danych osobowych i systemów ich przetwarzania". Wykaz ten zawiera następujące informacje:

1) nazwę zbioru danych,
2) określenie systemu przetwarzania danych osobowych,
3) lokalizację miejsca przetwarzania danych osobowych,
4) stosowane przy przetwarzaniu danych osobowych oprogramowanie,
5) precyzyjny zakres danych osobowych w systemie (pola i relacje pomiędzy nimi),
6) określenie pól informacyjnych w systemie,
7) określenie sposobu przepływu danych pomiędzy systemami,
8) wskazanie możliwość wydruku zakresu przetwarzania danych osobowych.

§5.

Przetwarzanie danych osobowych odbywa się na serwerze i na stacjach roboczych użytkowników.

§6.

1. W ramach procesów przetwarzania danych ma miejsce przepływ danych pomiędzy różnymi systemami informatycznymi. Informacje na temat przepływu danych pomiędzy różnymi systemami informatycznymi znajdują się w „Wykazie zasobów danych osobowych i systemów ich przetwarzania, o którym mowa w § 4".
2. Szczegółowe informacje dotyczące przepływu danych osobowych pomiędzy danymi systemami informatycznymi znajdują się w instrukcjach zarządzania danym systemem.

§ 7.

W systemie informatycznym obowiązują zabezpieczenia na poziomie podstawowym. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego znajduje się w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Naruszewie", stanowiącej załącznik nr 2 do Zarządzenia Wójta Gminy Naruszewo z dnia 5 kwietnia 2016 roku.

Rozdział III
Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

§ 8.

ADO powołuje Administratora Systemów Informatycznych (ASI), który przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania.

§ 9.

W celu realizacji powierzonych zadań ABI w Urzędzie ma prawo:

1) kontrolować komórki organizacyjne Urzędu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
2) wydawać polecenia kierownikom komórek organizacyjnych Urzędu w zakresie bezpieczeństwa danych osobowych;
3) informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych;
4) żądać od wszystkich pracowników Urzędu wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

§ 10.

Do obowiązków Lokalnych Administratorów Bezpieczeństwa Informacji należy w szczególności:

1) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez kierowane referaty lub na zajmowanym stanowisku;
2) występowanie z wnioskiem do ADO o nadanie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom;
3) zgłaszanie do ABI zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru;

4) udostępnianie danych osobowych innemu podmiotowi lub osobie, której dane dotyczą;
5) przestrzeganie obowiązków dotyczących obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń zbiorów;
6) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w kierowanym referacie, z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań wykonywanych przez te osoby przy przetwarzaniu danych osobowych i przekazywanie ABI aktualnej ewidencji tych osób wraz z priorytetami im przydzielonymi;
7) zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

§ 11.

Do obowiązków użytkowników danych osobowych należy w szczególności:
1) zapoznanie się i stosowanie obowiązujących przepisów prawa w zakresie ochrony danych osobowych,
2) zapewnienie bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem,
3) informowanie przełożonych o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych,
4) przestrzeganie tzw. „zasady czystego biurka" - na biurku powinny znajdować się jedynie dokumenty potrzebne do wykonania bieżącej pracy,
5) niszczenie zbędnych dokumentów papierowych oraz nośników zawierających dane osobowe w niszczarkach dokumentów lub umieszczania ich w specjalnie do tego celu przygotowanych pojemnikach,
6) dbanie o to, by dokumenty zawierające dane osobowe były przechowywane w zamkniętych szafach lub szufladach,
7) dbanie, aby osoby postronne (np. goście) poruszały się po pomieszczeniach, w których przetwarzane są dane osobowe tylko przy asyście osób zatrudnionych,
8) Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. Zaleca się ponadto szczególną ostrożność podczas ich transportu, a w szczególności stosowanie się do poniższych zasad:
9) nie wolno pozostawiać komputera przenośnego bez dozoru,
10) w samochodzie nie wolno przewozić komputera przenośnego umieszczonego na siedzeniu (komputer przenośny należy przewozić albo w zamkniętym bagażniku, albo na podłodze w miejscu przeznaczonym na nogi pasażera),
11) zabronione jest odstępowanie komputera przenośnego osobom trzecim.

§12.

1. Administrator Systemu Informatycznego odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu.
2. Do obowiązków ASI w zakresie ochrony danych osobowych należy w szczególności:
   1) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie;
   2) nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   3) nadzór nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych;

4) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Urzędzie w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych;
5) nadzór nad przesyłaniem danych osobowych drogą teletransmisji;
6) nadzór nad przestrzeganiem zasad bezpieczeństwa w przypadku udostępniania danych osobowych innym podmiotom drogą teletransmisji danych;
7) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
8) podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń;
9) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
10) podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.

Rozdział IV
Gromadzenie danych osobowych

§ 13.

Dane osobowe przetwarzane w Urzędzie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 14.

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 15.

W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem OchrDanychU albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział V
Przetwarzanie danych osobowych

§ 16.

1. W przypadku zgłoszenia przez Lokalnego Administratora Bezpieczeństwa Informacji zamiaru utworzenia nowego zbioru danych osobowych ABI przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, jeżeli takie zgłoszenie jest ustawowo wymagane, na podstawie obowiązującego wzoru zgłoszenia.
2. ASI, w uzgodnieniu z ABI, określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym, o których mowa w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO.
3. ABI sprawdza warunki techniczne dotyczące zabezpieczeń w systemie informatycznym opisane w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO; w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do ASI o podniesienie poziomu zabezpieczeń.

4. Przygotowany przez ABI projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO parafują Lokalny Administrator Bezpieczeństwa Informacji oraz ASI.
5. ABI przedkłada wniosek o rejestrację zbioru danych osobowych ADO i zgłasza go do GIODO.
6. Lokalny Administrator Bezpieczeństwa Informacji zgłasza – w terminie 5 dni – zmiany dotyczące przetwarzania danych w zarejestrowanym zbiorze danych osobowych do ABI.
7. ASI zgłasza – w terminie 5 dni – zmiany dotyczące sposobu przetwarzania danych osobowych oraz ich zabezpieczeń w systemie informatycznym do ABI.
8. ABI przygotowuje aktualizację zgłoszenia zbioru danych osobowych do GIODO w terminie 30 dni od dnia dokonania zmiany w zbiorze, na podstawie obowiązującego wzoru. Przepisy ust. 2–5 stosuje się odpowiednio.

Rozdział VI
Obowiązek informacyjny

§ 17.

1. Użytkownicy danych osobowych są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają, o:
   1) adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane,
   2) celu zbierania danych,
   3) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej,
   4) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania;
2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 OchrDanychU.
3. Wzór formularza stosowanego dla spełnienia obowiązków, o których mowa w ust. 1 i 2, stanowi załącznik nr 4 do Polityki Bezpieczeństwa.

§ 18.

1. Materiały dotyczące innej niż ustawowa działalności Urzędu mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.
2. Kandydaci do pracy w Urzędzie w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.
3. Dokumenty złożone przez kandydata wybranego w procesie rekrutacji, zostaną dołączone do jego akt osobowych.
4. Dokumenty złożone przez kandydatów, którzy nie zostali wybrani w procesie rekrutacji będą przechowywane zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 roku w sprawie instrukcji kancelaryjne, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 16, poz. 67 ze zm.).
5. Wzór formularza stosowanego dla spełnienia obowiązków wymienionych w ust. 2, stanowi załącznik 5 do Polityki Bezpieczeństwa Informacji.

Rozdział VII
Udostępnianie danych osobowych

§ 19.

1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub

podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

2. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów,
   2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
   3) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie nie dłuższym niż 30 dni od daty jego otrzymania.
6. Wniosek o udostępnienie przekazywany jest do Lokalnego Administratora Bezpieczeństwa Informacji, który podejmuje decyzję o udostępnieniu.
7. Lokalny Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

§ 20.

Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

Rozdział VIII
Ochrona przetwarzania danych osobowych

§ 21.

1. Do przetwarzania danych osobowych mogą być dopuszczeni pracownicy Urzędu posiadający upoważnienie nadane przez ADO. Wzór upoważnienia określa załącznik nr 6 do Polityki Bezpieczeństwa.
2. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 7 do Polityki Bezpieczeństwa.

§ 22.

ADO zobowiązany jest do zbierania, ewidencjonowania i przechowywania:

1) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych; wzór formularza oświadczenia stanowi załącznik nr 8 do Polityki Bezpieczeństwa;
2) porozumień zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej; wzór formularza porozumienia stanowi załącznik nr 9 do Polityki Bezpieczeństwa.

§ 23.

1. Dopuszcza się możliwość powierzenia przetwarzania danych osobowych zgodnie z art. 31 OchrDanychU.
2. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy zawartej na piśmie pomiędzy ADO a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
3. Lokalny Administrator Bezpieczeństwa Informacji informuje ABI o zamiarze powierzenia danych osobowych do przetwarzania.
4. ABI przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
5. W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.
6. Każda osoba delegowana do wykonywania zadań na rzecz Urzędu Gminy w Naruszewie, związanych z powierzeniem przetwarzania danych osobowych, obowiązana jest podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.
7. Projekt umowy parafują:
   1) ABI,
   2) Lokalny Administrator Bezpieczeństwa Informacji,
   3) ASI – jeżeli zlecenie czynności dotyczyć będzie przetwarzania danych w systemie informatycznym,
   4) radca prawny.
8. Zaparafowany projekt umowy jest przedkładany przez ABI do akceptacji i podpisu ADO.

Rozdział IX
Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

§ 24.

Przepisy niniejszego rozdziału stosuje się w przypadku:

1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych,
2) podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

§ 25.

Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

§ 26.

Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych,
2) nieautoryzowane modyfikacje lub zniszczenie danych,
3) udostępnienie danych nieautoryzowanym podmiotom,

4) nielegalne ujawnienie danych,
5) pozyskiwanie danych z nielegalnych źródeł.

§ 27.

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub ABI, a następnie postępować stosownie do podjętej przez niego decyzji.
2. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   1) opisanie działania wskazującego na naruszenie ochrony danych osobowych,
   2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
   3) wskazanie istotnych informacji mogących wskazywać na przyczynę naruszenia,
   4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 28.

1. ABI podejmuje działania mające na celu:
   1) minimalizację negatywnych skutków zdarzenia,
   2) wyjaśnienie okoliczności zdarzenia,
   3) zabezpieczenie dowodów zdarzenia,
   4) umożliwienie dalszego bezpiecznego przetwarzania danych.
2. Dla realizacji celów określonych w ust. 1 ABI ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:
   1) żądania wyjaśnień od pracowników,
   2) korzystania z pomocy konsultantów,
   3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§ 29.

Odmowa udzielenia wyjaśnień lub współpracy z ABI traktowana będzie jako naruszenie obowiązków pracowniczych.

§ 30.

ABI po opanowaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór raportu końcowego stanowi załącznik nr 10 do Polityki Bezpieczeństwa Informacji.

Wójt

mgr inż. Beata Pierścińska

Załącznik nr 1 do Polityki Bezpieczeństwa
w Urzędzie Gminy w Naruszewie

Wykaz pomieszczeń Urzędu Gminy w Naruszewie, w których przetwarzane są dane osobowe

	Lokalizacja Adres i numer budynku	Numer i przeznaczenie pomieszczenia*	Piętro	Nazwa referatu użytkującego pomieszczenie	Osoby pracujące w pomieszczeniu**	Zabezpieczenie pomieszczenia***
1.	2.	3.	4.	5.	6.	7.

*Należy podać numer pomieszczenia i jego przeznaczenie np. pokój biurowy, archiwum, kancelaria, serwerownia, biuro przepustek.
** Należy podać same stanowiska i liczbę osób bez imion i nazwisk.
*** Należy podać sposób zabezpieczenia pomieszczenia np. drzwi zamykane na klucz, kraty w oknach, pomieszczenie monitorowane, kontrola dostępu itp.

Załącznik nr 2 do Polityki Bezpieczeństwa
Urzędu Gminy w Naruszewie

Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

§ 1.

1. ABI, pracownicy zatrudnieni na samodzielnych stanowiskach pracy oraz kierownicy referatów Urzędu Gminy w Naruszewie odpowiadają za należyte zabezpieczenie fizyczne zasobów danych osobowych w podległych komórkach.
2. ABI zobowiązany jest przeprowadzać bezpośrednią kontrolę stanu zabezpieczeń fizycznych zbiorów danych osobowych oraz zgłaszać ADO uwagi lub propozycje kontroli.
3. Obszarem, w którym przetwarzane są dane osobowe, jest siedziba Urzędu Gminy w Naruszewie, Naruszewo 19a.
4. ABI jest odpowiedzialny za prowadzenie i uaktualnianie wykazu pomieszczeń, w których przetwarzane są dane osobowe.
5. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach, o których mowa w pkt 4, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą właściciela zasobów danych osobowych.
6. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru przetwarzania danych osobowych, o którym mowa w ust. 3. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych.
7. ABI może zezwolić na przebywanie w pomieszczeniach, o których mowa w pkt 4, osobom sprzątającym te pomieszczenia poza godzinami pracy Urzędu bez konieczności obecności osoby dopuszczonej do przetwarzania danych. Osoby sprzątające podpisują oświadczenie o zachowaniu poufności.
8. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
9. Lokalny Administrator Bezpieczeństwa Informacji zabezpiecza obszar przetwarzania danych zgodnie z pkt 8.
10. Budynek i pomieszczenia Urzędu Gminy w Naruszewie posiadają następujące zabezpieczenia:
    1) drzwi zewnętrzne zaopatrzone są w podwójne zamki patentowe,
    2) drzwi do pomieszczeń biurowych posiadają zamki zamykane na klucz,
    3) zasady postępowania z kluczami oraz zabezpieczenia budynku i pomieszczeń Urzędu Gminy w Naruszewie reguluje Instrukcja postępowania z kluczami oraz zabezpieczenia budynku Urzędu Gminy Naruszewo, pomieszczeń znajdujących się w budynku Urzędu Gminy i pomieszczeń gospodarczych znajdujących się poza budynkiem Urzędu Gminy wprowadzona Zarządzeniem Wójta Nr 11/10 z dnia 30 kwietnia 2010 roku,
    4) dokumenty z danymi osobowymi przechowywane są w szafach na akta wyposażonych w zamki zamykane na klucz,

5) system sygnalizacji alarmu i włamania, do którego szyfr posiadają: Wójt Gminy i wskazani pracownicy gospodarczy, jest podłączony do siedziby agencji ochrony,

§ 2.

1. W przypadku przetwarzania danych osobowych na urządzeniach przenośnych lub dokumentach papierowych poza obszarem wymienionym w § 1 pkt 3, należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych.
2. Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe, określa ASI w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Naruszewie".

§ 3.

1. Właściciele zasobów danych osobowych przekazują ABI:
   1) aktualny wykaz zasobów danych osobowych przetwarzanych w danej komórce organizacyjnej,
   2) wykaz osób upoważnionych do przetwarzania określonego zasobu danych osobowych,
   3) wykaz pomieszczeń, w których przetwarzany jest poszczególny zasób danych osobowych w podległej komórce organizacyjnej i ich zabezpieczeń.
2. Pracownik właściwy w sprawach kadrowych na bieżąco informuje ABI o:
   1) ustaniu zatrudnienia osoby w Urzędzie;
   2) przeniesieniu pracownika do innego referatu Urzędu, celem kontroli jego uprawnień do dostępu do danych osobowych.
3. ASI przekazuje ABI:
   1) aktualny wykaz systemów teleinformatycznych, w których przetwarzane są dane osobowe;
   2) informacje o programach zastosowanych do przetwarzania danych osobowych;
   3) sposób przepływu danych pomiędzy poszczególnymi systemami.
4. ABI ustala szczegółowe zakresy informacji oraz formę i tryb ich przekazywania.
5. Każda zmiana informacji w zakresie ujętym w pkt 1–3 wymaga bieżącej aktualizacji przez osoby wskazane w wymienionych punktach.
6. Na podstawie przekazywanych informacji ABI prowadzi aktualny wykaz zasobów danych osobowych przetwarzanych w Urzędzie.

Wójt

mgr inż. Beata Pierścińska

Załącznik nr 3 do Polityki Bezpieczeństwa
w Urzędzie Gminy w Naruszewie

...../.....

Wykaz zasobów danych osobowych i systemów ich przetwarzania

Lp.	Nazwa zbioru/zasobu danych osobowych	System przetwarzania /nazwa systemu	Lokalizacja miejsca przetwarzania	Zastosowane oprogramowanie	Pełny zakres danych osobowych w systemie*	Pola informacyjne w systemie**	Sposób przepływu danych pomiędzy systemami	Możliwość wydruku zakresu przetwarzanych danych osobowych
1.								
2.								

* Należy podać zakres upoważnienia związany z czynnościami przy przetwarzaniu danych osobowych: zbieranie danych, wprowadzanie danych pracowniczych, odczyt, zapis, modyfikacja, drukowanie, usuwanie/niszczenie.

** Należy podać identyfikator (id, login) dla każdego systemu, do którego dana osoba ma dostęp.

Załącznik nr 4 do Polityki Bezpieczeństwa
w Urzędzie Gminy w Naruszewie

...... /.....

OŚWIADCZENIE

Ja niżej podpisany(a) ..... oświadczam, iż zostałem(am) poinformowana przez pracownika Urzędu Gminy w Naruszewie o:

1) adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane;
2) celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
3) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania;
4) możliwości wniesienia żądania zaprzestania przetwarzania moich danych osobowych;
5) możliwości wniesienia sprzeciwu.

....
(Miejsce złożenia oświadczenia) (Data złożenia oświadczenia) (Numer PESEL)

.....
(Podpis osoby składającej)

Załącznik nr 5 do Polityki Bezpieczeństwa

....
(Pieczęć nagłówkowa urzędu) (Miejscowość, data)

Adresat.....
.....
.....

W związku z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2015 r. poz. 2135 ze zm.) uprzejmie Pana/Panią informuję, iż administratorem danych osobowych zawartych w przekazanych przez Pana/Panią dokumentach aplikacyjnych jest Urząd Gminy w Naruszewie, Naruszewo 19a.
Pana/Pani dane osobowe będą przetwarzane w celu przeprowadzenia procesu rekrutacyjnego oraz wybrania pracownika i zawarcia umowy o pracę. Dane osobowe nie będą udostępnianie innym podmiotom. Posiada Pan/Pani prawo dostępu do treści swoich danych oraz ich poprawiania. Zebrane dane osobowe zostały przez Panią/Pana podane dobrowolnie.

.....
(Podpis ADO)

Załącznik nr 6 do Polityki Bezpieczeństwa
w Urzędzie Gminy w Naruszewie

...../.....

Pan/Pani .....
zatrudniony/a w Urzędzie Gminy
w Naruszewie
na stanowisku .....

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 ze zm.)

upoważniam

Pana/Panią do przetwarzania danych osobowych oraz do obsługi systemu informatycznego funkcjonującego w Urzędzie Gminy w Naruszewie oraz urządzeń wchodzących w jego skład, służących przetwarzaniu danych osobowych, w zakresie niezbędnym do wykonywania obowiązków służbowych.

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych ma Pan/Pani obowiązek zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia.

Niniejsze upoważnienie:

1) zostało wydane na czas .....,
2) może być w każdym czasie cofnięte,
3) wygasa z dniem rozwiązania lub wygaśnięcia stosunku pracy z upoważnionym pracownikiem.

Otrzymuje:

.....

Załącznik nr 7 do Polityki Bezpieczeństwa
w Urzędzie Gminy w Naruszewie

...../.....

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy w Naruszewie

Lp.	Imię i nazwisko	Stanowisko/funkcja	Typ umowy/porozumienia				Zakres rzeczowy uprawnienia	Ramy czasowe	
			Pracownik	Współpracownik	Wolontariusz	Praktyka/Staż		od ...[1]	do ...[2]
1									
2									

[1] Data zatrudnienia lub nawiązania współpracy z daną osobą.
[2] Następny dzień roboczy po ustaniu zatrudnienia danej osoby lub zakończeniu z nią współpracy – wynika to z faktu, iż ostatniego dnia zatrudnienia/współpracy dana osoba może jeszcze musieć przetwarzać dane osobowe, wykonując swoje obowiązki stanowiskowe.

3									
4									
5									

Załącznik nr 8 do Polityki Bezpieczeństwa
w Urzędzie Gminy w Naruszewie

……/.....

OŚWIADCZENIE

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:

Rodzaj zadań	Właściwe zaznaczyć
Zadań i obowiązków wynikających z umowy o pracę zarówno w trakcie wykonywania umowy, jak i po jej rozwiązaniu	
Zadań wynikających z umowy cywilnoprawnej zarówno w trakcie wykonywania umowy, jak i po jej wygaśnięciu	
Zadań wynikających z umowy praktyki zarówno w trakcie wykonywania umowy, jak i po jej wygaśnięciu	

*właściwe zaznaczyć

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Gminy w Naruszewie dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia służbowego nie będę wykorzystywał(a) danych osobowych ze zbiorów Urzędu Gminy w Naruszewie

Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Urzędzie Gminy w Naruszewie zasadach dotyczących przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa Informacji.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami o ochronie danych osobowych oraz o grożącej, stosownie do przepisów rozdziału 8 ustawy o ochronie danych osobowych, odpowiedzialności karnej.

…… ……
(miejsce złożenia oświadczenia) (data złożenia oświadczenia)

……
(podpis osoby składającej oświadczenie)

Załącznik nr 9 do Polityki Bezpieczeństwa
w Urzędzie Gminy w Naruszewie

...../.....

Porozumienie zawierane pomiędzy Wójtem Gminy Naruszewo a pracownikiem zatrudnionym przy przetwarzaniu danych osobowych, w sprawie wykorzystania oddanego do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej

§ 1

Wójt Gminy Naruszewo, zwany dalej „Wójtem", oraz ..... (*wskazać imię i nazwisko pracownika*), zwany dalej „pracownikiem", zawierają na czas trwania zatrudnienia pracownika w Urzędzie Gminy w Naruszewie porozumienie w sprawie wykorzystania sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej.

§ 2

Wójt zobowiązuje się do:

1) zaznajomienia pracownika z obowiązującymi przy realizacji powierzonych mu zadań i obowiązków przepisami prawa i regulacjami wewnętrznymi, w szczególności związanymi z przetwarzaniem danych osobowych, przy wykorzystaniu sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej;
2) zapewnienia pracownikowi niezbędnego sprzętu informatycznego, w tym komputera, drukarki i urządzeń, umożliwiających komunikację dla prawidłowego i terminowego wykonywania zadań i obowiązków;
3) zapewnienia pracownikowi legalnego oprogramowania wspierającego realizację powierzonych mu zadań i obowiązków;
4) braku konsekwencji służbowych w przypadku nie wywiązania się pracownika z zadań i obowiązków spowodowanego niedziałaniem lub wadliwym działaniem sprzętu informatycznego, oprogramowania lub udostępnionych zasobów, chyba że działanie takie będzie wynikiem działania pracownika;
5) akceptowania wykorzystywania w miejscu pracy przez pracownika powierzonego mu sprzętu informatycznego, oprogramowania i zasobów sieciowych dla celów służących samokształceniu, w tym szczególnie podnoszenia kwalifikacji związanych z wykonywanymi zadaniami i pełnionymi obowiązkami, pod warunkiem wcześniejszego prawidłowego i terminowego wykonania powierzonych mu zadań i obowiązków.

§ 3

Pracownik zobowiązuje się do:

1) przestrzegania obowiązujących przepisów prawa i regulacji wewnętrznych w zakresie wykorzystania sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej podczas wykonywania swoich zadań i obowiązków, w tym w szczególności podczas przetwarzania danych osobowych;
2) wykorzystywania powierzonego mu sprzętu informatycznego, oprogramowania i zasobów sieciowych wyłącznie dla realizacji powierzonych mu zadań i obowiązków lub dla celów służących samokształceniu, w tym szczególnie podnoszenia kwalifikacji związanych z pełnionymi obowiązkami;

3) dbania o powierzony mu sprzęt informatyczny, oprogramowanie i zasoby sieciowe;
4) powstrzymania się od działań mogących mieć wpływ na bezpieczeństwo danych, w tym w szczególności od dokonywania jakichkolwiek zmian w konfiguracji powierzonego mu sprzętu informatycznego, od instalowania lub odinstalowania oprogramowania na powierzonym mu sprzęcie informatycznym oraz od wykorzystywania sprzętu lub oprogramowania do celów prywatnych, niezwiązanych w żaden sposób z wykonywanymi zadaniami i obowiązkami lub samokształceniem.

§ 4

Wójt informuje, a pracownik przyjmuje do wiadomości, że praca sieci informatycznej, sprzętu informatycznego, łączy teleinformatycznych i telekomunikacyjnych, działanie oprogramowania, przepływ danych i informacji oraz działania wszystkich pracowników związane z tymi elementami podlegają stałemu monitoringowi w celu zapewnienia bezpieczeństwa danych.

....

(podpis Wójta) (podpis pracownika)

Załącznik nr 10 do Polityki Bezpieczeństwa
W Urzędzie Gminy w Naruszewie

……/.....

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych
w Urzędzie Gminy w Naruszewie

1. Data: …… Godzina: ……

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……
……
……
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika, jeśli występuje)

3. Lokalizacja zdarzenia:

……
……
……..
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……
……
……
……
……

5. Przyczyny wystąpienia zdarzenia:
……
……
……
……
……
6. Podjęte działania:
……
……
……
……
7. Skutki zdarzenia:
……
……
……
……

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

8. Postępowanie wyjaśniające:

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

.....
(data, podpis ABI)

Załącznik nr 2
do zarządzenia nr 22/2016
Wójta Gminy Naruszewo
z dnia 5 kwietnia 2016 roku

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 Naruszewo.
2. Wójt Gminy wykonuje obowiązki administratora danych osobowych w odniesieniu do prowadzonych w Urzędzie Gminy Naruszewo zbiorów danych.
3. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się środki bezpieczeństwa na poziomie wysokim.

II
Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez przełożonego lub administratora bezpieczeństwa informacji z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w jednostce wewnętrznymi regulacjami w tym zakresie.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone, z zastrzeżeniem ust. 3, wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, wydane przez administratora danych osobowych.
3. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone również osoby, którym udzielono upoważnień do przetwarzania danych osobowych na podstawie porozumień zawartych w sprawie powierzenia przetwarzania danych osobowych.
4. Rejestracji użytkownika w systemie informatycznym przetwarzającym dane osobowe dokonuje administrator systemów informatycznych na wniosek przełożonego użytkownika, który zawiera:
   - imię i nazwisko użytkownika,
   - stanowisko zajmowane przez użytkownika,
   - nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
   - datę, z jaką ma nastąpić rejestracja.
5. Wyrejestrowania użytkownika z systemu informatycznego dokonuje na wniosek administratora danych osobowych lub przełożonego użytkownika administrator systemów informatycznych po uzgodnieniu z administratorem bezpieczeństwa informacji.

6. Wzór wniosku o rejestrację/wyrejestrowanie użytkownika w systemie informatycznym przetwarzającym dane osobowe stanowi załącznik nr 1 do niniejszej instrukcji.
7. Rejestracja w systemie informatycznym polega na wprowadzeniu do systemu identyfikatora, hasła oraz ustanowienia zakresu dostępnych danych i operacji dla każdego użytkownika.
8. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator systemów informatycznych.
9. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
10. Przełożeni użytkowników zobowiązani są pisemnie informować administratora danych osobowych lub administratora bezpieczeństwa informacji o każdej zmianie dotyczącej użytkowników mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych osobowych.
11. Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

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.
4. Użytkownik, z chwilą przystąpienia do pracy w systemie informatycznym, otrzymuje hasło początkowe i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy, na sobie tylko znany ciąg znaków.
5. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
6. System informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie najpóźniej 90 dni od dnia ostatniej jego zmiany.
7. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie jego ważności.
8. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie, użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.
9. Jeśli istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie je zmienić oraz powiadomić o tym fakcie.

IV
Administrator bezpieczeństwa informacji

1. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne oraz hasła.

V
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 systemów informatycznych w porozumieniu z administratorem bezpieczeństwa informacji.
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.
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:
   1) wylogować się z systemu informatycznego
   albo
   2) wywołać blokowany hasłem wygaszacz ekranu.
9. Kończąc pracę użytkownik jest obowiązany:
   1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
   2) zabezpieczyć stanowisko pracy.
10. Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się w szafach zamykanych na klucz.

VI
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 systemów informatycznych lub inna osoba przez niego wyznaczona.
3. W przypadku lokalnego przetwarzania danych osobowych na służbowych komputerach, użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych.
4. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegrywanie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze. Jeśli z przyczyn technicznych nie jest to możliwe, użytkownicy systemu są zobowiązani do sporządzania kopii zapasowych zbiorów danych na nośniku danych i przechowywania w szafie zamykanej na klucz.
5. 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 systemów informatycznych.

6. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
   1) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji i zapisywana na nośnikach danych;
   2) 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;
   3) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest raz w miesiącu.
7. Kopie zapasowe przechowywane są w szafie zamykanej na klucz.

VII
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 lub administratora bezpieczeństwa informacji.
2. Okresowe kopie zapasowe wykonywane są na dyskietkach, 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 bezpieczeństwa informacji oraz administrator systemów informatycznych.
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.

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

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator systemów informatycznych.
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 lub administratora bezpieczeństwa informacji.
6. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych" nadawców.
7. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
   Administrator systemów informatycznych jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   1) sieci lokalnej i rozległej;
   2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

IX
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.

X
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 pracowników zapewniających obsługę informatyczną Urzędu Gminy.
2. Administrator systemów informatycznych okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z administratorem bezpieczeństwa informacji.
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 systemów informatycznych.
5. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez pracowników zapewniających obsługę informatyczną Urzędu Gminy, 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 bezpieczeństwa informacji.

XI
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 systemów informatycznych.
2. Do czasu przybycia administratora systemów informatycznych na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych, należy:
   1) 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;
   2) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia;
   3) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;
   4) udokumentować wstępnie zaistniałe naruszenie;
   5) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia administratora systemów informatycznych lub administratora bezpieczeństwa informacji.
3. Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych administrator systemów informatycznych:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania;
   2) może żądać wyjaśnień dotyczących zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   3) dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia;
   4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia;
   5) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu administratora danych osobowych.
4. Po wyczerpaniu niezbędnych środków doraźnych, administrator systemów informatycznych 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:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób, które złożyły wyjaśnienia w związku z naruszeniem;
   2) określenie czasu i miejsca naruszenia oraz powiadomienia o naruszeniu;
   3) określenie rodzaju naruszenia i okoliczności mu towarzyszących;
   4) wyszczególnienie uwzględnionych przesłanek wyboru metody postępowania i opis podjętego działania;
   5) wstępną ocenę przyczyn wystąpienia naruszenia;
   6) ocenę przeprowadzonego postępowania wyjaśniającego i działań podjętych w celu usunięcia naruszenia i jego skutków.
6. Administrator danych osobowych przekazuje raport kierownikowi jednostki w terminie

14 dni od daty zdarzenia.

7. Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, administrator systemów informatycznych 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.

Wójt

mgr inż. Beata Pierścińska

Załącznik nr 1 do Instrukcji Zarządzania Systemem Informatycznym

....., dnia .....

.....

Wniosek
o rejestrację/wyrejestrowanie użytkownika w systemie informatycznym przetwarzającym dane osobowe

wnoszę o rejestrację/wyrejestrowanie

Pani/Pana
.....
Pracownika
.....
w systemie informatycznym przetwarzającym dane osobowe (nazwa zbioru danych osobowych oraz nazwa systemu informatycznego):
.....
.....
.....
od dnia .....

.....
(podpis przełożonego)