ZARZĄDZENIE NR 61/2016
WÓJTA GMINY GNIEWINO
z 3 października 2016 r.

w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych w jednostce, instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz innych potrzeb związanych z przetwarzaniem informacji w Urzędzie Gminy Gniewino.

Na podstawie art.36 i art.39a ustawy z 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2015r., poz.2135 ze zm.[1]), §3 w związku z §4 i §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz.1024) a także zgodnie z §20 rozporządzenia Rady Ministrów z 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012r. poz.526) oraz art.33 ust.3 ustawy z 8 marca 1990r. o samorządzie gminnym (Dz.U. z 2015r. poz.1515 ze zm.[2])

Wójt Gminy Gniewino
zarządza, co następuje:

§ 1.

Wprowadza się *Politykę Bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Gminy Gniewino*, stanowiącą załącznik nr 1 do zarządzenia.

§ 2.

Traci moc zarządzenie Wójta Gminy Gniewino Nr 90/2010 z 29 września 2010r. w sprawie ustalenia i wdrożenia polityki bezpieczeństwa informacji w Urzędzie Gminy Gniewino oraz Zarządzenie Wójta Gminy Gniewino Nr 92/2010 z 5 października 2010r. w sprawie wprowadzenia w Urzędzie Gminy Gniewino Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
mgr Zbigniew Walczak

[1] Zmieniony Dz. U. z 2015 r., poz. 2281
[2] Zmieniony Dz.U. z 2015 r., poz. 1045; Dz.U. z 2015 r., poz. 1890

Załącznik nr 1 Zarządzenia Nr 61/2016
Wójta Gminy Gniewino z 3 października 2016 r.

POLITYKA BEZPIECZEŃSTWA

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Gminy Gniewino, określa zasady przetwarzania danych osobowych, oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych, oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1. **ZBIORZE DANYCH** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. **PRZETWARZANIU DANYCH** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. **SYSTEMIE INFORMATYCZNYM** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. **ZABEZPIECZENIU DANYCH W SYSTEMIE INFORMATYCZNYM** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. **USUWANIU DANYCH** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. **ADMINISTRATORZE DANYCH** - rozumie się przez to Wójta Gminy Gniewino.

§ 3

Administrator Danych w Urzędzie Gminy Gniewino nie wyznacza **Administratora Bezpieczeństwa Informacji**.

§ 4

Wzór wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik A do „Polityki Bezpieczeństwa".**

§ 5

Wzór wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik B do „Polityki Bezpieczeństwa".**

§ 6

W Urzędzie Gminy Gniewino dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 7

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez

Administratora Danych. Administrator Danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. **Administrator Danych** nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie upoważnienia, którego wzór stanowi **załącznik C do „Polityki Bezpieczeństwa"**. Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – jej wzór stanowi **załącznik D** do „Polityki Bezpieczeństwa".
2. Zestawienie danych osobowych - kiedy i przez kogo zostały do zbioru wprowadzone, oraz komu są przekazywane – jego wzór stanowi **załącznik E** do „Polityki Bezpieczeństwa".
3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – **załącznik F** do „Polityki Bezpieczeństwa".

§ 8

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

§ 9

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

§ 10

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje **INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM** będąca **załącznikiem G** do „Polityki Bezpieczeństwa".

§ 11

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

§ 12

DEKLARACJA INTENCJI, CELE I ZAKRES POLITYKI BEZPIECZEŃSTWA

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.
2. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.
3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne), oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

5. Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.

7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
   b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
   d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.

8. Dla skutecznej realizacji Polityki **Administrator Danych** zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne,
   b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
   c) kontrolę i nadzór nad przetwarzaniem danych osobowych,
   d) monitorowanie zastosowanych środków ochrony,
   e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa,
   f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.

9. Monitorowanie przez **Administratora Danych** zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

10. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów ustawy, oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

Załącznik A do Załącznika nr 1 Zarządzenia Nr 61/2016
Wójta Gminy Gniewino z 3 października 2016 r.

Wykaz budynków, pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe
- zgodnie z §4 pkt. 1 Rozporządzenia Ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r.

Lp.	*Referat*	*Nr pokoju/ pomieszczenia*	*Rodzaj zastosowanego zabezpieczenia pomieszczenia*	*Uwagi*

Data i podpis Administratora Danych Osobowych

.....

Załącznik B do Załącznika nr 1 Zarządzenia Nr 61/2016
Wójta Gminy Gniewino z 3 października 2016 r.

Wykaz
zbiorów danych osobowych gromadzonych i przetwarzanych
w Urzędzie Gminy w Gniewinie
- zgodnie, z § 4 pkt 2, 3 i 4 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.
(zbiór jest zbiorem otwartym podlegającym zmianom)

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania danych *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	Opis struktury zbiorów danych	Sposób przepływu danych pomiędzy poszczególnymi systemami
1.				
2.				
3.				
4.				
5.				

Data i podpis Administratora Danych Osobowych

.....

Załącznik C do Załącznika nr 1 Zarządzenia Nr 61/2016
Wójta Gminy Gniewino z 3 października 2016r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

zgodnie z Art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

ZGIGNIEW WALCZAK –WÓJT GMINY GNIEWINO jako Administrator Danych Osobowych
nadaje upoważnienie do przetwarzania danych osobowych
w Urzędzie Gminy Gniewino, dla:

IMIĘ I NAZWISKO: .....

.....

STANOWISKO SŁUŻBOWE: .....

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z:

- **POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH**
- **ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY**

Upoważnienie nadaje się do ustania stosunku pracy. Wszelakie poprzednie upoważnienia do przetwarzania danych osobowych z dniem wprowadzenia niniejszego wygasają. Jednocześnie bieżące upoważnienie zostaje zawieszone w przypadku nieobecności / urlopu przekraczającego 30 dni kalendarzowych. Po upływie w/w okresu nieobecności / urlopu upoważniony(a) wykonując obowiązki wynikające z upoważnienia otrzymuje ponowne upoważnienie niniejszym dokumentem.

Ja niżej podpisany/a zobowiązuję się do przestrzegania zasad panujących w w/w podmiocie w zakresie ochrony danych osobowych, a w szczególności **„Polityki Bezpieczeństwa"** i **„Instrukcji Zarządzania Systemem Informatycznym"** oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Zobowiązuję się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w w/w podmiocie oraz sposobów zabezpieczeń, a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Przyjmuję do wiadomości, iż jestem zobligowana/y do zmiany hasła dostępu do stanowiska pracy (komputera) w terminie co 30 dni kalendarzowych. Hasło musi być niepowtarzalne względem wcześniejszego, oraz składać się z 8 znaków (w tym małe, duże litery oraz znak specjalny).

Oświadczam, iż zapoznałem(am) się i akceptuję zasady dotyczące korzystania z sieci informatycznej na terenie w/w podmiotu, a mianowicie:

1. Mając na uwadze wysoką sprawność oraz elastyczność kształtowania procesów w pracy, pracodawca zastrzega sobie prawo do archiwizacji, monitorowania oraz przekierowywania służbowej poczty elektronicznej.
2. Pracodawca informuje, że wszystkie połączenia internetowe wykonane w sieci w/w podmiotu są rejestrowane, zgodnie z wymogami ustawy Prawa Telekomunikacyjnego.
3. Pracodawca zastrzega sobie również prawo monitorowania w/w połączeń oraz żądania wyjaśnień w zakresie realizowanej przez pracownika aktywności w sieci oraz do dowolnego kształtowania zakresu dostępu do sieci internetowej.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016r. poz. 195) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 ze zm.).

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

.....
[podpis Administratora Danych Osobowych]

.....
[podpis upoważnionego]

Załącznik D do Załącznika nr 1 Zarządzenia Nr 61/2016
Wójta Gminy Gniewino z 3 października 2016r.

EWIDENCJA OSÓB PRZETWARZAJĄCYCH DANE W PODMIOCIE POSIADAJĄCYCH UPOWAŻNIENIE

zgodnie z Art. 39. 1. Ustawy o ochronie danych osobowych z 29 sierpnia 1997r.

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)

ADMINISTRATOR DANYCH OSOBOWYCH

.....

(data i czytelny podpis Administratora Danych Osobowych)

Załącznik E do Załącznika nr 1 Zarządzenia Nr 61/2016
Wójta Gminy Gniewino z 3 października 2016r.

ZESTAWIENIE DANYCH OSOBOWYCH Z INFORMACJĄ KIEDY I PRZEZ KOGO ZOSTAŁY DO ZBIORU WPROWADZONE ORAZ KOMU SĄ PRZEKAZYWANE

zgodnie z art. 38 Ustawy o ochronie danych osobowych z 29 sierpnia 1997r.

LP.	RODZAJ UDOSTĘPNIONYCH DANYCH OSOBOWYCH	DATA WPROWADZENIA DANYCH DO ZBIORU	DATA PRZEKAZANIA DANYCH OSOBOWYCH	IMIĘ I NAZWISKO OSOBY KTÓRA OTRZYMAŁA DANE	CEL PRZEKAZANIA DANYCH OSOBOWYCH
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

ADMINISTRATOR DANYCH OSOBOWYCH

.....

(czytelny podpis Administratora Danych Osobowych)

Załącznik F do Załącznika nr 1 Zarządzenia Nr 61/2016
Wójta Gminy Gniewino z 3 października 2016r.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

zgodnie z §4 pkt 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004r.

Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

ŚRODKI OCHRONY FIZYCZNEJ DANYCH:

a) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nieprzeciwpożarowymi).

b) Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.

c) Pomieszczenia, w których przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.

d) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.

e) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.

f) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

g) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

ŚRODKI OCHRONY TECHNICZNEJ DANYCH:

a) Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.

b) Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

c) Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.

d) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

e) Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.

f) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.

g) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

h) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

i) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

j) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

ŚRODKI ORGANIZACYJNE:

a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.

c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

e) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy o ochronie danych osobowych.
W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą.
Wszystkie osoby upoważnione do przetwarzania danych osobowych mogę ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

Załącznik G do Załącznika nr 1 Zarządzenia Nr 61/2016
Wójta Gminy Gniewino z 3 października 2016r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Zgodnie z **ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI**
z 29 kwietnia 2004r.
w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Ilekroć w „Instrukcji" jest mowa o:

1. **PODMIOCIE** — rozumie się przez to Urząd Gminy Gniewino,
2. **USTAWIE** — rozumie się przez to ustawę z 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2014r. poz.1182, 1662, z 2015r. poz. 1309), zwaną dalej „ustawą",
3. **IDENTYFIKATORZE UŻYTKOWNIKA** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
4. **HAŚLE** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
5. **SIECI TELEKOMUNIKACYJNEJ** — rozumie się przez to sieć telekomunikacyjną w rozumieniu art.2 pkt 35 ustawy z 16 lipca 2004r. — Prawo telekomunikacyjne (Dz.U. z 2014r., poz.243, 827, 1198, z 2015r. poz. 1069),
6. **SIECI PUBLICZNEJ** — rozumie się przez to termin, który przywołuje §2 ust.5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004r. (Dz.U. z 2004r. Nr 100, poz.1024),
7. **TELETRANSMISJI** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
8. **ROZLICZALNOŚCI** — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
9. **INTEGRALNOŚCI DANYCH** — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
10. **RAPORCIE** — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
11. **POUFNOŚCI DANYCH** — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
12. **UWIERZYTELNIANIU** — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

W Urzędzie Gminy Gniewino za przestrzeganie zapisów „instrukcji" odpowiedzialny jest **Administrator Danych.**

§ 2

W związku z tym, że w Urzędzie Gminy Gniewino urządzenia systemu informatycznego, służącego do przetwarzania danych osobowych, połączone są z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia, wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim,** a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Danych Osobowych. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

   w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
   - poprzez zainstalowanie programu antywirusowego o nazwie: **ESET ANTYWIRUS**
   - poprzez zainstalowanie firewall (zapora sieciowa),
   - poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem,
2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich

danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień.

4. Kopie zapasowe:

   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym: DYSK SIECIOWY – PRZECHOWYWANY W DZIALE KSIĘGOWOŚCI / KOPIA ZAPASOWA PRZECHOWYWANA W SEJFIE W POKOJU GŁÓWNEJ KSIĘGOWEJ.

   b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

   a) daty pierwszego wprowadzenia danych do systemu,

   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,

   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,

   d) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

   e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w §7 ust. 1 pkt 1,2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w §7 ust. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024).

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w §7 ust. 1 pkt. 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024), mogą być realizowane w jednym z nich, lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 minut, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§ 5

Administrator Danych ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok.

§ 6

W przypadku stwierdzenia przez **Administratora Danych** uchybień dotyczących przetwarzania danych w podmiocie powinien wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7

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