BURMISTRZ
TRZEMESZNA

Zarządzenie Nr 245/2016
Burmistrza Trzemeszna
z dnia 18 sierpnia 2016 roku

w sprawie: ustalenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym systemów informatycznych służącym do przetwarzania danych osobowych w Urzędzie Miejskim Trzemeszna

Na podstawie §3 ust.3, §4 oraz § 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 z 2004r.)

zarządzam co następuje:

§1. Ustala się politykę bezpieczeństwa stanowiącą załącznik Nr 1 oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim Trzemeszna, która stanowią załączniki Nr 2 do niniejszego zarządzenia.

§2. Zobowiązuje się pracowników Urzędu Miejskiego Trzemeszna do stosowania zasad określonych w polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym.

§3. Wykonanie zarządzenia powierza się koordynatorowi ds. ochrony danych osobowych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

§ 5. Traci moc Zarządzenie Nr 341/2013 Burmistrza Miasta i Gminy Trzemeszno z dnia 27 września 2013 roku w sprawie: ustalenia Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym systemów informatycznych służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Trzemesznie.

BURMISTRZ
Krzysztof Derezińiski

Załącznik Nr 1 do Zarządzenia Nr 245/2016 Burmistrza Trzemeszna z dnia 18 sierpnia 2016 roku

POLITYKA BEZPIECZEŃSTWA

Administrator Danych – **KRZYSZTOF DEREZIŃSKI**

dnia **18 sierpnia 2016 r.** w podmiocie o nazwie: **GMINA TRZEMESZNO**

zgodnie z **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)

wdraża dokument o nazwie „Polityka Bezpieczeństwa". Zapisy tego dokumentu wchodzą w życie

z dniem **18 sierpnia 2016 r**.

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w podmiocie: **GMINA TRZEMESZNO**, 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 organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2014r., poz. 1182, 1662, z 2015 r. poz. 1309), decydujące o celach i środkach przetwarzania danych osobowych,
7. **KOORDYNATORZE OCHRONY DANYCH OSOBOWYCH** – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony danych osobowych,
8. **PODMIOCIE** – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nieposiadający osobowości prawnej, jednostkę budżetową.

§ 3

Administrator Danych w podmiocie o nazwie: **GMINA TRZEMESZNO** , wyznacza **KOORDYNATORA OCHORNY DANYCH OSOBOWYCH** celem nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Upoważnienie dla **KOORDYNATORA OCHORNY DANYCH OSOBOWYCH**, oraz zakres obowiązków określa wzór **załącznika do „Polityki Bezpieczeństwa" nr 1.**

§ 4

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa wzór **załącznika do „Polityki Bezpieczeństwa" nr 2.**

§ 5

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa wzór **załącznika do „Polityki Bezpieczeństwa" nr 3.**

§ 6

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa wzór **załącznika do „Polityki Bezpieczeństwa" nr 4.**

§ 7

W podmiocie 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.

§ 8

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 na podstawie upoważnień. Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:

1. Wzór ewidencji osób przetwarzających dane w podmiocie posiadających upoważnienie – stanowi **załącznik nr 5** do „Polityki Bezpieczeństwa".

2. Wzór zestawienia danych osobowych - kiedy i przez kogo zostały do zbioru wprowadzone, oraz komu są przekazywane – stanowi **załącznik nr 6** do „Polityki Bezpieczeństwa".

3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych –wzór stanowi **załącznik nr 7** do „Polityki Bezpieczeństwa".

§ 9

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.

§ 10

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.

§ 11

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje **INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**.

§ 12

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.**

§ 13

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.

Administrator Danych Osobowych

BURMISTRZ
Krzysztof Derezliński

.....
Podpis

KOORDYNATOR OCHORNY DANYCH OSOBOWYCH

.....
Podpis

TRZEMESZNO, DNIA ..... R.

UPOWAŻNIENIE DLA KOORDYNATORA OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES OBOWIĄZKÓW

załącznik nr 1 do „Polityki Bezpieczeństwa"

Na podstawie § 3 Polityki Bezpieczeństwa z dnia ..... zgodnie z założeniami
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

Na podstawie art. 36a ust. 1 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2014 r. poz. 1182, 1662, z 2015 r. poz. 1309)

Administrator Danych Osobowych (ADO): ----------

powołuje w podmiocie: ----------

o numerze NIP: ----------

Koordynator ds. Ochrony Danych Osobowych ----------

o numerze Pesel: ----------

Upoważnienie jest ważne od chwili podpisania przez strony do dnia wycofania upoważnienia przez **Administratora Danych Osobowych.**

Do zadań Koordynatora Ochrony Danych Osobowych należy wsparcie Administratora Danych Osobowych w zakresie:

1. zapewnianie przestrzegania przepisów o ochronie danych osobowych,
2. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 u.o.d.o., zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 u.o.d.o. zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Koordynator Ochrony Danych Osobowych wspiera Administratora Danych Osobowych w nadzorze, opracowaniu i aktualizowaniu dokumentacji, o której mowa w art. 36 ust. 2 u.o.d.o., oraz przestrzegania zasad w niej określonych, przestrzeganie w podmiocie zapisów Instrukcji Zarządzania Systemem Informatycznym. Koordynator ochrony danych osobowych wspiera Administratora Danych Osobowych w prowadzenia wszelkiej dokumentacji opisującej sposób przetwarzania danych w podmiocie, a w szczególności:

zgodnie z § 4. „Polityki Bezpieczeństwa"

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

osobowe, który określa załącznik do „Polityki Bezpieczeństwa" nr 2,

zgodnie z § 5. „Polityki Bezpieczeństwa"

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa" nr 3,

zgodnie z § 6. „Polityki Bezpieczeństwa"

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa" nr 4,

zgodnie z § 8. „Polityki Bezpieczeństwa"

Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 6 do „Polityki Bezpieczeństwa" oraz zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – załącznik nr 7 do „Polityki Bezpieczeństwa".

Koordynator ds. Ochrony Danych Osobowych wspiera Administratora Danych Osobowych w zakresie sprawdzenia zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje sprawozdania dla GIODO zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Koordynator ds. Ochrony Danych Osobowych zapewnia zapoznanie się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator Danych Osobowych zapewnia środki i organizacyjną odrębność Koordynatora do spraw Danych Osobowych - niezbędne do należytego wykonywania przez niego zadań wynikających z niniejszego upoważnienia i przepisów ustawy.

OŚWIADCZENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako, **Koordynator ds. Ochrony Danych Osobowych** będę nadzorował przestrzeganie zasad ochrony danych w podmiocie o nazwie: **GMINA TRZEMESZNO** , zgodnie z obowiązkami wynikającymi z tego upoważnienia, oraz ustawy o ochronie danych osobowych.

Administrator Danych Osobowych	**Koordynator ds. Ochrony Danych Osobowych**
----------	----------
Podpis	**Podpis**

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

Załącznik do „Polityki Bezpieczeństwa" nr 2 zgodnie z § 4 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

LP.	DOKŁADNY ADRES (NP. ADRES SIEDZIBY FIRMY GDZIE PRZETWARZANE SĄ DANE)	DZIAŁ UŻYTKUJĄCY POMIESZCZENIE	NR POKOJU LUB POMIESZCZENIA	RODZAJ ZASTOSOWANEGO ZABEZPIECZENIA POMIESZCZENIA	UWAGI
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					

Data i podpis Administratora Danych Osobowych

.....

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

załącznik do „Polityki Bezpieczeństwa" nr 3 zgodnie, z § 4 pkt 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Uwagi**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			

Data i podpis Administratora Danych Osobowych

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami - załącznik do „Polityki Bezpieczeństwa" nr 4 zgodnie, z § 4 pkt 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Struktura zbiorów *(np. imię i nazwisko, e-mail, telefon itd.)*	Przepływ danych (np. wydruk danych z internetu)	Uwagi
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

Data i podpis Administratora Danych Osobowych

EWIDENCJA OSÓB PRZETWARZAJĄCYCH DANE W PODMIOCIE POSIADAJĄCYCH UPOWAŻNIENIE

Załącznik nr 5 do „Polityki Bezpieczeństwa" zgodnie z Art. 39. 1. Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

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)
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						

ADMINISTRATOR DANYCH OSOBOWYCH

.....

(data i czytelny podpis Administratora Danych Osobowych)

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

Załącznik nr 6 do „Polityki Bezpieczeństwa" zgodnie z art. 38 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

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.					
11.					

ADMINISTRATOR DANYCH OSOBOWYCH

.....

(czytelny podpis Administratora Danych Osobowych)

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

Załącznik do „Polityki Bezpieczeństwa" nr 7 zgodnie z § 4 pkt 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

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

2. **Koordynator ds. Ochrony Danych Osobowych** wraz z wyznaczonymi Użytkownikami przeprowadzają okresową analizę ryzyka dla systemu i na tej podstawie przedstawiają Administratorowi Danych propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.

3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje **Koordynator ds. Ochrony Danych Osobowych**.

4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

5. Środki ochrony, zastosowane przez **Koordynator ds. Ochrony Danych Osobowych** dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
   - środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
   - środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS);
   - środki organizacyjne (np. powołanie ABI, utworzenie Instrukcji zarządzania systemem informatycznym);

6. Zastosowane środki:

ŚRODKI OCHRONY FIZYCZNEJ DANYCH:

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

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

c) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.

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

e) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie, lub kasie pancernej.

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.

7. ŚRODKI OCHRONY TECHNICZNEJ DANYCH:

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

b) Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.

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

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) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.

g) Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej serwerów.

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

i) Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.

j) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.

k) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

l) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

8. 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.

ADMINISTRATOR DANYCH OSOBOWYCH

.....
(data i czytelny podpis Administratora Danych Osobowych)

Załącznik Nr 2 do Zarządzenia Nr 245/2016 Burmistrza Trzemeszna z dnia 18 sierpnia 2016 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych – **KRZYSZTOF DEREZIŃSKI**
w podmiocie o nazwie: **GMINA TRZEMESZNO**

Zgodnie z **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
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją". Zapisy tego dokumentu wchodzą w życie z dniem 18 sierpnia 2016 R.

Ilekroć w „Instrukcji" jest mowa o:

1. **PODMIOCIE** — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nieposiadający osobowości prawnej, jednostkę budżetową,
2. **USTAWIE** — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182, 1662, z 2015 r. 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 dnia 16 lipca 2004 r. — 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 dnia 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.

Załącznik Nr 2 do Zarządzenia Nr 245/2016 Burmistrza Trzemeszna z dnia 18 sierpnia 2016 roku

§ 1

W podmiocie o nazwie: **GMINA TRZEMESZNO** , za przestrzeganie zapisów „instrukcji" odpowiedzialny jest **Administrator Danych** lub zgodnie z zapisem §3 „Polityki Bezpieczeństwa" wyznaczony **Koordynator ds. Ochrony Danych Osobowych.**

§ 2

W związku z tym, że w podmiocie o nazwie: **GMINA TRZEMESZNO** przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest 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, **Koordynatora ds. Ochrony Danych Osobowych** 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: **Kasperski Endpoint Protection**
   - 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: tj. serwerownia oraz w pok. Nr 2b w budynku Urzędu Miejskiego przy ul. Gen. H. Dąbrowskiego zaopatrzonymi w system alarmowy.
   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

Koordynator ds. Ochrony Danych Osobowych lub inne osoby przez niego wskazane mają obowiązek dokonywania przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbania o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych **Koordynator ds. Ochrony Danych Osobowych** ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§ 6

W przypadku stwierdzenia przez **Koordynatora ds. Ochrony Danych Osobowych** uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz 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 dnia 29 sierpnia 1997 r. 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.**

Administrator Danych Osobowych

BURMISTRZ

Krzysztof Derezinski

.....

Podpis

Koordynator ds. Ochrony Danych Osobowych

.....

Podpis