Zarządzenie Nr 35/ 15

Wójta Gminy Brudzeń Duży z dnia 16 czerwca 2015r.

w sprawie

wprowadzenia i wdrożenia do stosowania Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w Urzędzie Gminy Brudzeń Duży

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z póź. Zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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) zarządzam, co następuje:

§1

Wprowadzam do stosowania Politykę Bezpieczeństwa Danych Osobowych stanowiącą załącznik nr 1 do niniejszego Zarządzenia oraz Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiącą załącznik nr 2 niniejszego Zarządzenia.

§2

Kierowników komórek organizacyjnych zobowiązuję do zapoznania podległych pracowników z powyżej wskazaną dokumentacją.

§3

Traci moc Zarządzenie nr 159/2008 w sprawie: Polityki bezpieczeństwa w Urzędzie Gminy w Brudzeniu Dużym oraz Zarządzenie nr 160/2008 w sprawie: Instrukcji zarządzania systemami informatycznymi w Urzędzie Gminy w Brudzeniu Dużym

§4

Zarządzenie wchodzi w życie z dniem podpisania i podlega ogłoszeniu.

POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY BRUDZEŃ DUŻY

Administrator Danych Osobowych - Andrzej Dwojnych Wójt Gminy Brudzeń Duży

dnia 16 czerwca 2015r. w podmiocie o nazwie **Urząd Gminy Brudzeń Duży**

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 16 czerwca 2015r.

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Gminy Brudzeń Duży 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, dostępnych 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, decydujące o celach i środkach przetwarzania danych osobowych,
7.administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.
8.podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3.

Administrator Danych w podmiocie Urząd Gminy Brudzeń Duży wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Upoważnienie dla **Administratora Bezpieczeństwa Informacji** oraz zakres obowiązków określa **załącznik do „Polityki Bezpieczeństwa" nr 1**

§ 4.

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

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik 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 **załącznik do „Polityki Bezpieczeństwa" nr 4**

§ 7.

Administratora Bezpieczeństwa Informacji dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować 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** lub **Administratora Bezpieczeństwa Informacji**. **Administrator Bezpieczeństwa Informacji** jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Bezpieczeństwa Informacji nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"**. Administrator Bezpieczeństwa Informacji prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 6** do „Polityki Bezpieczeństwa"

2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – **załącznik nr 7** do „Polityki Bezpieczeństwa"

§ 9.

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

§ 10.

Administrator Bezpieczeństwa Informacji 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**

Podpis Administratora Danych Osobowych

.....

Podpis

Podpis Administratora Bezpieczeństwa Informacji

.....

Podpis

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych Osobowych - Andrzej Dwojnych Wójt Gminy Brudzeń Duży

dnia 16 czerwca 2015r. w podmiocie o nazwie **Urząd Gminy Brudzeń Duży**

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 16 czerwca 2015r.

Ilekroć w „instrukcji" jest mowa o:

1) podmiocie — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, 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 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
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

Za przestrzeganie w podmiocie **Urząd Gminy Brudzeń Duży** zapisów „instrukcji" odpowiedzialny jest Administrator danych oraz wyznaczony Administrator Bezpieczeństwa Informacji.

§2

W związku z tym, że w podmiocie **Urząd Gminy Brudzeń Duży** 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, Administratora Bezpieczeństwa Informacji 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 Bezpieczeństwa Informacji. 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.

•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 – w pokoju nr 11.

zaopatrzonym 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:

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

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

3) 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:

1) daty pierwszego wprowadzenia danych do systemu;

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że

dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna

osoba;

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

4) 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;

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

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, 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 ust.1

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, 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 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Bezpieczeństwa Informacji 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. W przypadku stwierdzenia usterek technicznych **Administrator Bezpieczeństwa Informacji** ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§6

W przypadku stwierdzenia przez **Administratora Bezpieczeństwa Informacji** 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**

Podpis Administratora Danych Osobowych

.....

Podpis

Podpis Administratora Bezpieczeństwa Informacji

.....

Podpis

Brudzeń Duży, 16 czerwca 2015r.

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

załącznik nr 1 do „Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Gminy Brudzeń Duży"

Na podstawie § 2. Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Gminy Brudzeń Duży z dnia 16 czerwca 2015r. 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 oraz na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285)

Administrator Danych Osobowych: Andrzej Dwojnych

powołuje w podmiocie: Urząd Gminy Brudzeń Duży,

NIP: 774 197 73 29

Administratora Bezpieczeństwa Informacji : Dariusz Reczek.

Pesel: 59080805175

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

Administrator Bezpieczeństwa Informacji jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. **Administrator Bezpieczeństwa Informacji** jest zobowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1. **Administrator Bezpieczeństwa Informacji** nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa".**

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przestrzeganie w podmiocie zapisów Instrukcji Zarządzania Systemem Informatycznym. **Administrator Bezpieczeństwa Informacji** prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

zgodnie z § 3. „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 § 4. „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 § 5. „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 § 7. „Polityki Bezpieczeństwa"

Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 6 do „Polityki Bezpieczeństwa"

Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – załącznik nr 7 do „Polityki Bezpieczeństwa"

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako administrator bezpieczeństwa informacji, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie - Urząd Gminy Brudzeń Duży zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji

.....

Podpis

Administrator Danych

.....

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	Urząd Gminy Brudzeń Duży				
2	Urząd Gminy Brudzeń Duży				
3	Urząd Gminy Brudzeń Duży				
4	Urząd Gminy Brudzeń Duży				
5	Urząd Gminy Brudzeń Duży				
6	Urząd Gminy Brudzeń Duży				
7	Urząd Gminy Brudzeń Duży				
8	Urząd Gminy Brudzeń Duży				
9	Urząd Gminy Brudzeń Duży				
10	Urząd Gminy Brudzeń Duży				
11	Urząd Gminy Brudzeń Duży				
12	Urząd Gminy Brudzeń Duży				

Lp.	**Dokładny adres** *(np. adres siedziby firmy gdzie przetwarzane są dane)*	**Dział użytkujący pomieszczenie**	**Nr pokoju lub pomieszczenia**	**Rodzaj zastosowanego zabezpieczenia pomieszczenia**	**Uwagi**
13	Urząd Gminy Brudzeń Duży				

Data i podpis Administratora Bezpieczeństwa Informacji : .....

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**

Data i podpis Administratora Bezpieczeństwa Informacji : .....

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 zblorów** *(np. imię i nazwisko, e-maii, telefon itd.)*	**Przepływ danych** (np. wydruk danych z internetu)	**Uwagi**

Data i podpis Administratora Bezpieczeństwa Informacji

.....

Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa" zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Dariusz Reczek - jako Administrator Bezpieczeństwa Informacji dnia 17 czerwca 2015r. nadaje upoważnienie do przetwarzania danych osobowych w podmiocie **Urząd Gminy Brudzeń Duży** dla:

Imię i nazwisko: .....

Adres zamieszkania: .....

Nr PESEL: .....

Stanowisko służbowe: .....

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

.....

.....

.....

.....

.....

.....

.....

Upoważnienie nadaje się bezterminowo –do czasu odwołania.

Upoważniony zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa" oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego obowiązuje tajemnica dotycząca danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń.

Administrator Bezpieczeństwa Informacji

.....

Podpis

Użytkownik

.....

Podpis

Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie

załącznik nr 6 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)*

Data i podpis Administratora Bezpieczeństwa Informacji

.....

Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

załącznik nr 7 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

Data i podpis Administratora Bezpieczeństwa Informacji

.....