Zarządzenie Nr 4/2018
Wójta Gminy Miedzichowo
z dnia 02 stycznia 2018 r.

w sprawie aktualizacji dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych.

Na podstawie art. 36a ust. 2 pkt. 1b ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) 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. z 2004 r. Nr 100, poz. 1024) zarządza się, co następuje:

§1. Zaktualizować i wprowadzić jako obowiązującą dokumentację opisującą sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych w postaci:
- Polityki Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Miedzichowo stanowiącej załącznik nr 1 do niniejszego zarządzenia
- Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Miedzichowo stanowiącej załącznik nr 2 do niniejszego zarządzenia

§2. Zarządzenie jest adresowane do pracowników podmiotu: Urząd Gminy Miedzichowo wykonujących czynności określone w „Polityce Bezpieczeństwa" oraz „Instrukcji Zarzadzania Systemem Informatycznym". Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią „Polityki Bezpieczeństwa" i „Instrukcji Zarządzania Systemem Informatycznym".

§3. Administrator Danych Osobowych: Urząd Gminy Miedzichowo zobowiązuje wszystkich pracowników do przestrzegania zapisów „Polityki Bezpieczeństwa" oraz stosowania się do „Instrukcji Zarządzania Systemem Informatycznym" pod groźbą konsekwencji służbowych, przewidzianych prawem.

§4. Traci moc zarządzenie Nr 11/K//2010 z dnia 30 kwietnia 2010 roku w sprawie wdrożenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędzie Gminy Miedzichowo oraz Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Miedzichowo

§5. Niniejsze zarządzenie wchodzi w życie z dniem podpisania i ogłoszenia tj. z dniem 02-01-2018 r.

WÓJT GMINY
MIEDZICHOWO
64-361 Miedzichowo
Ul. Poznańska 12

WÓJT
dr Stanisław Piechota

....

(podpis Administratora Danych Osobowych)

RADCA PRAWNY
Renata [illegible]

POLITYKA BEZPIECZEŃSTWA

Administrator Danych Osobowych – **Urząd Gminy Miedzichowo**
w osobie: **Stanisław Piechota** dnia **02-01-2018 r.**

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 **02-01-2018 r.**

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w podmiocie: **Urząd Gminy Miedzichowo,** 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) **ADMINISTRATORZE BEZPIECZEŃSTWA INFORMACJI** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
2) **ADMINISTRATORZE DANYCH OSOBOWYCH** – rozumie się przez to Administratora Danych Osobowych podmiotu reprezentowanego przez osobę kierującą,
3) **ADMINISTRATORZE SYSTEMU INFORMATYCZNEGO** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków administratora systemu,
4) **HAŚLE** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
5) **IDENTYFIKATORZE** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
6) **INTEGRALNOŚCI DANYCH** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7) **ODBIORCY DANYCH** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
8) **OSOBIE UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH** – rozumie się przez to osobę,

która upoważniona została do przetwarzania danych osobowych przez Administratora Danych Osobowych na piśmie zgodnie z art. 37 ustawy,

9) **POUFNOŚCI DANYCH** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

10) **PRZETWARZAJĄCYM** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

11) **RAPORCIE** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

12) **ROZLICZALNOŚCI** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

13) **ROZPORZĄDZENIU** – rozumie się przez to 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),

14) **SIECI PUBLICZNEJ** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. nr 100, poz. 1024),

15) **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. 2016 poz. 1489 z późn. zm.),

16) **SERWISANCIE** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego i oprogramowania,

17) **SYSTEMIE INFORMATYCZNYM ADMINISTRATORA DANYCH** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

18) **TELETRANSMISJI** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

19) **USTAWIE** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922),

20) **UWIERZYTELNIANIU** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

21) **UŻYTKOWNIKU** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

§ 3

Administrator Danych Osobowych o nazwie: **Urząd Gminy Miedzichowo,** potwierdza wyznaczenie **Administratora Bezpieczeństwa Informacji** celem nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. **Upoważnienie dla Administratora Bezpieczeństwa Informacji**, oraz zakres obowiązków określa **ZAŁĄCZNIK NR 1** do „Polityki Bezpieczeństwa".

§ 4

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

§ 5

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi wraz z przepływem danych pomiędzy poszczególnymi systemami określa **ZAŁĄCZNIK NR 3** do „Polityki Bezpieczeństwa".

§ 6

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.

§ 7

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych Osobowych. Administrator Danych Osobowych** 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. Osobom, które nie przetwarzają danych osobowych, ale mają dostęp do obszaru przetwarzania danych osobowych, **Administrator Danych Osobowych** wydaje **zgody na przebywanie w obszarze przetwarzania – ZAŁĄCZNIK NR 4** do „Polityki Bezpieczeństwa". **Administrator Danych Osobowych** nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **ZAŁĄCZNIK NR 5** do „Polityki Bezpieczeństwa". Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:

1. ewidencja osób posiadających upoważnienie do przetwarzania danych osobowych, oraz przebywania w obszarze przetwarzania w podmiocie – **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".
3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – **ZAŁĄCZNIK NR 8** do „Polityki Bezpieczeństwa".

§ 8

Administrator Danych Osobowych 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. Wzór umowy powierzenia danych osobowych określa **ZAŁĄCZNIK NR 9** do „Polityki Bezpieczeństwa".
Jeżeli **Administrator Danych Osobowych** nie powierza danych osobowych innemu podmiotowi, ale istnieją przesłanki na okoliczność zobowiązania drugiej strony do konieczności zachowania powziętych informacji

w tajemnicy, stosuje się klauzulę poufności. Wzór klauzuli poufności określa **ZAŁĄCZNIK NR 10**.

§ 9

Na wniosek osoby, której dane dotyczą, **Administrator Danych Osobowych** jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji. Poza tym, Administrator Danych Osobowych w związku z art. 24 ust. 1, art. 25 ust. 1 i art. 32 ust. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2016 roku poz. 922) jest zobowiązany spełniać **obowiązek informacyjny**, którego treść określa **ZAŁĄCZNIK NR 11** do „Polityki Bezpieczeństwa".

§ 10

Administrator Danych Osobowych 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 Osobowych 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 bezpieczeństwa 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 Osobowych** 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 Osobowych** 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 Osobowych 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

.....

Podpis

Administrator Bezpieczeństwa Informacji

.....

Podpis

Miedzichowo, dnia 02-01-2018 r.

UPOWAŻNIENIE DLA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI ORAZ ZAKRES OBOWIĄZKÓW

załącznik nr 1 do „Polityki Bezpieczeństwa"

Na podstawie § 3 Polityki Bezpieczeństwa z dnia **02-01-2018 r.**, 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 2016 r. poz. 922 z późn. zm.)

Administrator Danych Osobowych (ADO): ***Urząd Gminy Miedzichowo***

o numerze NIP: ***596-12-09-353***

w osobie ***Stanisław Piechota***

potwierdza powołanie :

Administratora Bezpieczeństwa Informacji (ABI): ***Marcin Cichowski***

o numerze Pesel: ***78062207899***

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

Zgodnie z art. 36a ust. 2 **do zadań ABI należy**:

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).

Administrator Bezpieczeństwa Informacji nadzoruje opracowanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2 u.o.d.o., oraz przestrzegania zasad w niej określonych. 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 § 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,

Miedzichowo, dnia 02-01-2018 r.

UPOWAŻNIENIE DLA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI ORAZ ZAKRES OBOWIĄZKÓW

załącznik nr 1 do „Polityki Bezpieczeństwa"

Na podstawie § 3 Polityki Bezpieczeństwa z dnia **02-01-2018 r.,** 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 2016 r. poz. 922 z późn. zm.)

Administrator Danych Osobowych (ADO): ***Urząd Gminy Miedzichowo***

o numerze NIP: ***596-12-09-353***

w osobie ***Stanisław Piechota***

potwierdza powołanie :

Administratora Bezpieczeństwa Informacji (ABI): ***Marcin Cichowski***

o numerze Pesel: ***78062207899***

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

Zgodnie z art. 36a ust. 2 **do zadań ABI należy**:

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).

Administrator Bezpieczeństwa Informacji nadzoruje opracowanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2 u.o.d.o., oraz przestrzegania zasad w niej określonych. 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 § 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 oraz posiadających upoważnienie do przebywania w obszarze przetwarzania - 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".

Administrator Bezpieczeństwa Informacji sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla Administratora Danych Osobowych, lub na wniosek GIODO zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Administrator Bezpieczeństwa Informacji zapewnia zapoznanie się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator Danych Osobowych zapewnia środki i organizacyjną odrębność Administratora Bezpieczeństwa Informacji - 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 **Administrator Bezpieczeństwa Informacji**, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie o nazwie: **Urząd Gminy Miedzichowo**, zgodnie z obowiązkami wynikającymi z tego upoważnienia, oraz ustawy o ochronie danych osobowych.

Oświadczam, że spełniam wymogi dotyczące osoby powołanej na stanowisko **Administratora Bezpieczeństwa informacji** tj.:

- nie byłem(am) karany(a) za umyślne przestępstwo,
- posiadam pełną zdolność do czynności prawnych, oraz korzystam z pełni praw publicznych,
- posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Administrator Danych Osobowych

WÓJT
dr Stanisław Piechota

.....

Podpis

Administrator Bezpieczeństwa Informacji

.....

Podpis

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 oraz posiadających upoważnienie do przebywania w obszarze przetwarzania - 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".

Administrator Bezpieczeństwa Informacji sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla Administratora Danych Osobowych, lub na wniosek GIODO zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Administrator Bezpieczeństwa Informacji zapewnia zapoznanie się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator Danych Osobowych zapewnia środki i organizacyjną odrębność Administratora Bezpieczeństwa Informacji - 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 **Administrator Bezpieczeństwa Informacji**, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie o nazwie: **Urząd Gminy Miedzichowo**, zgodnie z obowiązkami wynikającymi z tego upoważnienia, oraz ustawy o ochronie danych osobowych.

Oświadczam, że spełniam wymogi dotyczące osoby powołanej na stanowisko **Administratora Bezpieczeństwa informacji** tj.:

- nie byłem(am) karany(a) za umyślne przestępstwo,
- posiadam pełną zdolność do czynności prawnych, oraz korzystam z pełni praw publicznych,
- posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Administrator Danych Osobowych

WÓJT
dr Stanisław Piechota

Podpis

Administrator Bezpieczeństwa Informacji

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 Miedzichowo Ul. Poznańska 12, 64-361 Miedzichowo	Referat Księgowości i Finansów	1,2,4,5	Drzwi zamykane na klucz, Szafy zamykane na klucz	Brak
		Referat Spraw Obywatelskich	3		
		Referat Organizacyjny	10,12,13,18		
		Wójt Gminy	11		
		Referat Infrastruktury i Ochrony Środowiska	14,19,100,102		
		Urząd Stanu Cywilnego	18		
		Samodzielne stanowisko ds. wojskowych i obronnych, OC i PPoż oraz Ewidencjonowania Materiałów Niejawnych	15		

Data i podpis Administratora Danych Osobowych

2018-01-02 .....WÓJT dr Stanisław Piechota.....

ZAŁĄCZNIK NR 3 DO POLITYKI BEZPIECZEŃSTWA:

- WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH zgodnie z § 4 pkt 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004
- OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI 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.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
1.	**PRACOWNICY**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **KADRY+ I PŁACE+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.**	IMIĘ, NAZWISKO, E-MAIL, TELEFON, ADRES ZAMELDOWANIA I ZAMIESZKANIA, ŚCIEŻKA ZAWODOWA, ŚCIEŻKA EDUKACYJNA, NR KONTA BANKOWEGO, NR NIP, PESEL, SERIA I NR DOWODU OSOBISTEGO, DATA URODZENIA, MIEJSCE URODZENIA, IMIONA RODZICÓW.	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
2.	**UMOWY CYWILNOPRAWNE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **KADRY+ I PŁACE+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.**	IMIĘ, NAZWISKO, E-MAIL, TELEFON, ADRES ZAMELDOWANIA I ZAMIESZKANIA, NR KONTA BANKOWEGO, NR NIP, PESEL, SERIA I NR DOWODU OSOBISTEGO, DATA URODZENIA, MIEJSCE URODZENIA, IMIONA RODZICÓW.	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
3.	**KANDYDACI DO PRACY**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, ADRES ZAMELDOWANIA, NR TELEFONU, DATA I MIEJSCE URODZENIA, PRZEBIEG PRACY	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
4.	**EWIDENCJA PODATNIKÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **POGRUN+ i WIP+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.**	IMIĘ I NAZWISKO, ADRES ZAMELDOWANIA, NR KONTA BANKOWEGO ,PESEL, NUMER NIP, SERIA I NR DOWODU OSOBISTEGO, NR TELEFONU, DATA URODZENIA, MIEJSCE URODZENIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
5.	**EWIDENCJA UPOMNIEŃ I TYTUŁÓW WYKONAWCZYCH**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **WIP+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.**	IMIĘ I NAZWISKO, ADRES ZAMELDOWANIA, NR KONTA BANKOWEGO ,PESEL, NUMER NIP, IMIĘ OJCA, IMIĘ MATKI, DATA URODZENIA, MIEJSCE URODZENIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
6.	**ZWROT PODATKU AKCYZOWEGO**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **POGRUN+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.**	IMIĘ I NAZWISKO, ADRES ZAMELDOWANIA, NR KONTA BANKOWEGO ,PESEL, NUMER NIP, SERIA I NR DOWODU OSOBISTEGO, NR TELEFONU, POWIERZCHNIA UŻYTKÓW ROLNYCH	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	

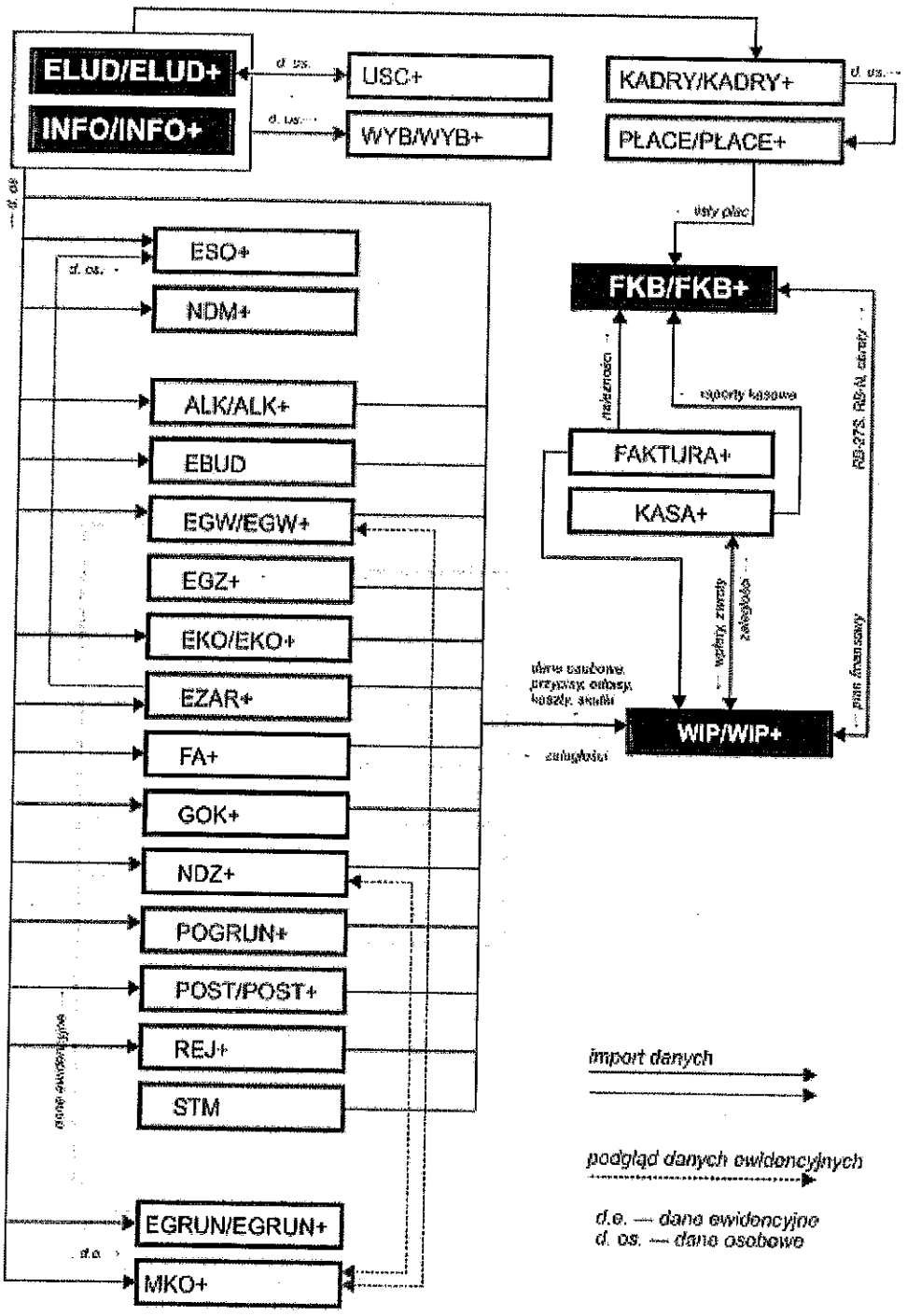
LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa <--> wersja elektroniczna)	UWAGI
7.	**BANKOWOŚĆ ELEKTRONICZNA**	WERSJA TRADYCYJNA (PAPIEROWA) +PROGRAM SPECJALISTYCZNY: **SYSTEM ECORPONET, PRZEGLĄDARKA INTERNETOWA**	IMIĘ I NAZWISKO, ADRES ZAMELDOWANIA, NR KONTA BANKOWEGO	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
8.	**DZIENNIK KORESPONDENCYJNY**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWA I ADRES FIRMY,, IMIĘ, NAZWISKO, ADRES OSOBY FIZYCZNEJ, NR TELEFONU	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
9.	**ARCHIWUM ZAKŁADOWE**	WERSJA TRADYCYJNA (PAPIEROWA)	IMIĘ, NAZWISKO, NR KONTA BANKOWEGO, NR NIP, PESEL, SERIA I NR DOWODU OSOBISTEGO, DATA URODZENIA, MIEJSCE URODZENIA, IMIONA RODZICÓW I UPOSAŻONYCH, ZAWÓD, WYKSZTAŁCENIE, NR TELEFONU, MIEJSCE PRACY	WERSJA PAPIEROWA	
10.	**KSIĘGI STANU CYWILNEGO**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **TECHNIKA PBUSC**	IMIĘ I NAZWISKO, IMIONA RODZICÓW, , DATA URODZENIA, MIEJSCE URODZENIA , MIEJSCE PRACY, ZAWÓD, WYKSZTAŁCENIE, ADRES ZAMIESZKANIA, PESEL, SERIA I NR DOWODU, NR TELEFONU	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
11.	**ZMIANA IMION I NAZWISK**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE +	IMIĘ I NAZWISKO, IMIONA RODZICÓW, , DATA I MIEJSCE URODZENIA , ADRES ZAMIESZKANIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
12.	**REJESTR MIESZKAŃCÓW I WYBORCÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: ELUD+ I WYB+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.	IMIĘ, NAZWISKO, ADRES ZAMELDOWANIA I ZAMIESZKANIA, PESEL, SERIA I NR DOWODU OSOBISTEGO, DATA URODZENIA, MIEJSCE URODZENIA, IMIONA RODZICÓW, WYKSZTAŁCENIE, PRZYPISANIE DO OBWODU I OKRĘGU WYBORCZEGO, UPRAWNIENIA WYBORCZE	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
13.	**SPRAWY DOTYCZĄCE ZAJĘCIA PASA DROGOWEGO**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, ADRES ZAMIESZKANIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
14.	**SPRAWY DOTYCZĄCE USUNIĘCIA DRZEW I KRZEWÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, ADRES ZAMIESZKANIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
15.	**GMINNE ODPADY KOMUNALNE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: ELUD+ I WYB+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.	IMIĘ, NAZWISKO, ADRES ZAMIESZKANIA, PESEL, NR KONTA BANKOWEGO,	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
16.	**WNIOSKI O UDOSTĘPNIENEI INFORMACJI PUBLICZNEJ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, ADRES ZAMIESZKANIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
17.	**REJESTR OSÓB PODLEGAJĄCYCH SŁUŻBIE WOJSKOWEJ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, ADRES ZAMIESZKANIA, SERIA I NR DOWODU OSOBISTEGO, DATA URODZENIA, MIEJSCE URODZENIA, IMIONA RODZICÓW	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
18.	**OŚWIADCZENIA MAJĄTKOWE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, ADRES ZAMIESZKANIA, DATA URODZENIA, MIEJSCE URODZENIA, MIEJSCE ZATRUDNIENIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
19.	**PRACOWNICY MŁODOCIANI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, PESEL, ADRES ZAMIESZKANIA, DATA URODZENIA, MIEJSCE URODZENIA, MIEJSCE ZATRUDNIENIA, NUMER KONTA BANKOWEGO	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
20.	**REALIZACJA OBOWIĄZKU NAUKI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, PESEL, ADRES ZAMIESZKANIA, DATA URODZENIA, MIEJSCE URODZENIA, MIEJSCE NAUKI	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
21.	**AWANS ZAWODOWY NAUCZYCIELI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, PESEL, ADRES ZAMIESZKANIA,	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
22.	**FUNDUSZ ALIMENTACYJNY ORAZ ZALICZKA ALIMENTACYJNA**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: FA+ i WIP+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.	IMIĘ I NAZWISKO, IMIONA RODZICÓW, , DATA URODZENIA, MIEJSCE URODZENIA , MIEJSCE PRACY, ADRES ZAMIESZKANIA, PESEL, SERIA I NR DOWODU, NR TELEFONU, NUMER NIP, ZAWÓD, WYKSZTAŁCENIE	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
23.	**ŚWIADCZENIA RODZINNE I ŚWIADCZENIE WYCHOWAWCZE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: EZAR+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.	IMIĘ I NAZWISKO, IMIONA RODZICÓW, , DATA URODZENIA, MIEJSCE URODZENIA , ADRES ZAMIESZKANIA, PESEL, NR TELEFONU, NR KONTA BANKOWEGO	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
24.	**DODATKI MIESZKANIOWE I DODATEK ENERGETYCZNY**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: NDM+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.	IMIĘ I NAZWISKO, IMIONA RODZICÓW, ADRES ZAMIESZKANIA, PESEL, NR TELEFONU, NR KONTA BANKOWEGO, SERIA I NR DOWODU OSOBISTEGO	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
25.	**STYPENDIA**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: ESO+ firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.	IMIĘ I NAZWISKO, IMIONA RODZICÓW, DATA I MIEJSCE URODZENIA, ADRES ZAMIESZKANIA, PESEL, NR TELEFONU, NR KONTA BANKOWEGO, NR NIP, MIEJSCE PRACY RODZICÓW,	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	

Data i podpis Administratora Danych Osobowych

2018-01-02 .....

WÓJT
dr Stanisław Piechota



Przepływ danych pomiędzy systemami pakietu firmy RADIX Spółka z ograniczoną odpowiedzialnością Sp.k.

EWIDENCJA OSÓB POSIADAJĄCYCH UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ PRZEBYWANIA W OBSZARZE PRZETWARZANIA

Załącznik nr 6 do „Polityki Bezpieczeństwa" zgodnie z Art. 39. 1. Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

* (z uwzględnieniem osób nieprzetwarzających dane osobowe, ale przebywających w pomieszczeniach, w których zachodzi proces przetwarzania danych osobowych)

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	RODZAJ UPOWAŻNIENIA (PRZETWARZANIE / PRZEBYWANIE)	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)
1.	Stanisław Piechota	Wójt Gminy Miedzichowo	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	Wojt
2.	Mirosława Kuryś	Skarbnik Gminy	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	mkurys
3.	Anna Mizgajska	Stanowisko ds. windykacji podatkowej, podatków od środków transportowych	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	amizgajska
4.	Urszula Janowska	Stanowisko ds. podatków i opłat	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	ujanowska
5.	Katarzyna Różańska	Główna Księgowa	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	krozanska

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	RODZAJ UPOWAŻNIENIA (PRZETWARZANIE / PRZEBYWANIE)	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)
6.	Emilia Grześkowiak	Stanowisko ds. pomocy rodzinie	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	egrzeskowiak
7.	Małgorzata Nikolin	Stanowisko ds. świadczeń wychowawczych oraz fundusz alimentacyjny	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	mnikolin
8.	Ilona Piosik	Stanowisko ds. księgowości budżetowej gminy	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	ipiosik
9.	Bogusława Wajman	Kierownik Referatu Infrastruktury i Ochrony Środowiska	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	Bwajman
10.	Ewa Nikolin-Kowalkowska	Stanowisko ds. płac	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	enikolin
11.	Kazimiera Włodarczyk	Stanowisko obsługi sekretariatu	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	kwlodarczyk

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	RODZAJ UPOWAŻNIENIA (PRZETWARZANIE / PRZEBYWANIE)	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)
12.	Zbigniew Piróg	Stanowisko ds. dróg publicznych i zamówień publicznych i inwestycji komunalnych	(PRZETWARZANIE / ~~PRZEBYWANIE~~)	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	zpirog
13.	Karolina Łotecka	Sekretarz Gminy	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	sekretarz
14.	Patrycja Stachowiak	Stanowisko ds. promocji gminy i kancelarii ogólnej	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	promocja
15.	Zbigniew Oses	Stanowisko ds. wojskowych i obronnych, obrony cywilnej i ochrony przeciwpożarowej	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	zoses
16.	Ewa Wieczorek	Kierownik USC Kierownik Referatu Spraw Obywatelskich	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	ewieczorek
17.	Anna Kowala	Stanowisko ds. obsługi organów gminy, ewidencji działalności gospodarczej i kadr	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	akowala

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	RODZAJ UPOWAŻNIENIA (PRZETWARZANIE / PRZEBYWANIE)	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)
18.	Paweł Krzywda	Stanowisko ds. gospodarki gruntami i gospodarki mieniem gminnym, gospodarowanie mieszkaniowym zasobem gminy	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	pkrzywda
19.	Mateusz Wesoły	Stanowisko ds. gospodarki przestrzennej gminy	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	mwesoly
20.	Alina Frańska	Stanowisko ds. pozyskiwania środków unijnych	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	afranska
21.	Beata Hartwig	Sprzątaczka	~~(PRZETWARZANIE /~~ PRZEBYWANIE	2018-01-02	DO USTANIA STOSUNKU PRACY		
22.	Mieczysław Petrykowski	Pracownik gospodarczy	~~(PRZETWARZANIE /~~ PRZEBYWANIE	2018-01-02	DO USTANIA STOSUNKU PRACY		
23.	Renata Kubaj	Stanowisko ds. ochrony środowiska	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-01-02	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	rkubaj
24.	Stefania Lisek	Stanowisko ds. gospodarki gruntami i gospodarki mieniem gminnym, gospodarowanie mieszkaniowym zasobem gminy	(PRZETWARZANIE / ~~PRZEBYWANIE~~	2018-02-10	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	slisek

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	RODZAJ UPOWAŻNIENIA (PRZETWARZANIE / PRZEBYWANIE)	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)
25.	Magdalena Juszczak	Stanowisko ds. windykacji podatkowej, podatków od środków transportowych	**(PRZETWARZANIE / ~~PRZEBYWANIE~~)**	2018-03-01	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	mjuszczak
26.	Anna Napierała	Młodszy referent	**(PRZETWARZANIE / ~~PRZEBYWANIE~~)**	2018-03-01	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	anapierala

ADMINISTRATOR DANYCH OSOBOWYCH

WÓJT
dr Stanisław Piechota

.....

(czytelny podpis Administratora Danych Osobowych)

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
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					

ADMINISTRATOR DANYCH OSOBOWYCH

WÓJT
dr Stanisław Piechota

.....

(czytelny podpis Administratora Danych Osobowych)

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

Załącznik do „Polityki Bezpieczeństwa" nr 8 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. ABI 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 ABI.

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 ABI 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) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy.

c) 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 stacjonarnego jak i przenośnego.

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

c) Zastosowano urządzenia typu UPS, 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.

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

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

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

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

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

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

n) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

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

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

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

WÓJT
dr Stanisław Piechota

.....

(data i czytelny podpis Administratora Danych Osobowych)

DOKUMENT WZORCOWY

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH NR .....

Załącznik do umowy Nr .....

Zawarta w dniu ..... r. w ..... pomiędzy:

[NAZWA INSTYTUCJI ORAZ ADRES]

zwanym w dalszej części niniejszej umowy „**Zleceniodawcą**"

reprezentowanym przez:

[IMIĘ I NAZWISKO]

---

a

[NAZWA INSTYTUCJI ORAZ ADRES]

zwanym w dalszej części niniejszej umowy „**Wykonawcą**"

reprezentowanym przez:

[IMIĘ I NAZWISKO]

---

o następującej treści:

§ 1

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. W związku z realizacją umowy nr ..... z dnia **[DATA]** r. pomiędzy **[PEŁNA NAZWA ZLECENIODAWCY]** a **[PEŁNA NAZWA WYKONAWCY]** ,o **[NAZWA ŚWIADCZONEJ USŁUGI]**. **Zleceniodawca** powierza **Wykonawcy** trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. z 2016 r. poz. 922 z późn. zm) zwanej dalej ,,ustawą" przetwarzanie danych osobowych.
2. **Zleceniodawca** oświadcza, że jest Administratorem Danych, które powierza.
3. Powierzone dane zawierają informacje typu: **[NP. DANE PRACOWNICZE]**.
4. **Zleceniodawca** powierza **Wykonawcy** przetwarzanie danych osobowych w zakresie określonym w § 2.

§ 2

ZAKRES I CEL PRZETWARZANIA DANYCH

1. **Wykonawca** będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych/:
   a) imię i nazwisko,
   b) numer ewidencyjny PESEL,
   c) seria i numer dowodu osobistego,
   d) ..... .
2. Celem przetwarzania danych jest **[NP. REALIZACJA OBSŁUGI KADROWO-PŁACOWEJ]**.
3. Zakres przetwarzania obejmuje: **wprowadzanie, wgląd, modyfikację, drukowanie, usuwanie, archiwizację, przesyłanie** **([1])** danych osobowych.
4. Powierzone przez **Zleceniodawcę** dane osobowe będą przetwarzane przez **Wykonawcę** wyłącznie w celu wykonywania przez **Wykonawcę** na rzecz **Zleceniodawcy** usług szczegółowo opisanych w umowie, o której mowa w § 1 ust.1 i w sposób zgodny z niniejszą Umową.

§ 3

SPOSÓB WYKONANIA UMOWY W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

1. **Wykonawca** zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 36 – 39a ustawy.
2. **Wykonawca** oświadcza, że 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 informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024):
   a) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
   b) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają określony w Rozporządzeniu poziom bezpieczeństwa,

([1]) niepotrzebne wykasować

c) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca,

d) do wykonania czynności objętych umową dopuszcza jedynie osoby posiadające imienne upoważnienia wraz z klauzulą poufności i posiadające odpowiednią wiedzę z zakresu ochrony danych osobowych.

3. **Wykonawca** zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

4. **Wykonawca** zobowiązuje się niezwłocznie zawiadomić **Zleceniodawcę** o:

   a) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa, a w szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,

   b) każdym nieupoważnionym dostępie do danych osobowych,

   c) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.

5. **Zleceniodawca** ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez **Wykonawcę**, oraz żądania składania przez niego pisemnych wyjaśnień.

6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel **Zleceniodawcy** sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. **Wykonawca** może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.

7. **Wykonawca** zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.

8. **Wykonawca** zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie **Zleceniodawcy** dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.

9. **Wykonawca** może „pod powierzyć" usługi objęte umową, o której mowa w § 1 ust. 1 i niniejszą umową podwykonawcom jedynie za zgodą **Zleceniodawcy**.

§ 4

ODPOWIEDZIALNOŚĆ WYKONAWCY

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie, ujawnienie, przekazanie osobom nieupoważnionym.

2. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§ 5

CZAS OBOWIĄZYWANIA UMOWY POWIERZENIA

1. Niniejsza Umowa powierzenia zostaje zawarta na czas określony:
   - od dnia **[DATA]** do dnia **[DATA]**.

§ 6

WARUNKI WYPOWIEDZENIA I ROZWIĄZANIA UMOWY

1. **Zleceniodawca** ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy **Wykonawca**:
   a) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
   b) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody **Zleceniodawcy**,
   c) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
   d) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.

2. Rozwiązanie niniejszej Umowy przez **Zleceniodawcę** jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.

3. **Wykonawca**, w przypadku wygaśnięcia umowy, o której mowa §1 ust.1 niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym **Zleceniodawcy** protokołem.

§8

POSTANOWIENIA KOŃCOWE

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu cywilnego.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby **Zleceniodawcy**.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

---------- za Zleceniodawcę

---------- za Wykonawcę

KLAUZULA POUFNOŚCI INFORMACJI

§ 1

Strony umowy zobowiązują się wzajemnie do nie wykorzystywania, nie ujawniania oraz nie przekazywania informacji, które stanowią tajemnicę przedsiębiorstwa drugiej strony niniejszej umowy.

§ 2

Strony powinny zachować poufność informacji, które zdobędą na każdym etapie jakiejkolwiek wzajemnej współpracy.

§ 3

Klauzula poufności danych obowiązuje strony przez okres trwania umowy, a także bezwzględnie po jej zakończeniu przez okres ..... lat.

§ 4

Strony odpowiadają za zachowanie powyższych informacji w tajemnicy przez osoby, którym wykonanie swoich obowiązków powierzyły.

§ 5

Strony umowy zobowiązują się do wykorzystywania przetwarzanych przez nie danych osobowych, w ramach realizacji niniejszej umowy, wyłącznie w celach określonych w umowie.

§ 6

Stronom umowy przysługuje każdym czasie i bez ograniczenia kontrola procesu przetwarzania i ochrony danych osobowych.

§ 7

Strony, dopełniając czynności wynikających z niniejszej umowy, zobowiązują się do przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016r. poz. 922 z późn. zm.)

§ 8

W przypadku nie dochowania warunków umowy, strony zastrzegają sobie prawo rozwiązania niniejszej umowy w trybie natychmiastowym, w każdym czasie.

TREŚĆ OBOWIĄZKU INFORMACYJNEGO ADMINISTRATORA DANYCH OSOBOWYCH

Urząd Gminy Miedzichowo
Ul. Poznańska 12, 64-361 Miedzichowo

reprezentowanym przez:

Stanisław Piechota

Zgodnie z art. 24 ust. 1 i art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 roku poz. 922) informuję, iż administratorem Pani/Pana danych osobowych jest **Urząd Gminy Miedzichowo ul. Poznańska 12, 64-361 Miedzichowo.**

Pani/Pana dane osobowe przetwarzane będą w celu np. przeprowadzenia postępowania rekrutacyjnego na wolne stanowisko pracy np. Młodszy Referent do obsługi sekretariatu. Pana/Pani dane osobowe nie będą udostępniane innym odbiorcom danych za wyjątkiem wypadków obowiązkowego udzielenia informacji określonych w przepisach szczególnych. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania. Podaje Pani/Pan swoje dane osobowe dobrowolnie.

Klauzula o ochronie danych osobowych

Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb niezbędnych do realizacji procesu rekrutacji (zgodnie z Ustawą z dnia 29.08.1997 roku o Ochronie Danych Osobowych; tekst jednolity: Dz. U. 2016 r. poz. 922).

- Wiem, że Administratorem danych osobowych jest Urząd Gminy Miedzichowo, ul. Poznańska 12, 64-361 Miedzichowo, reprezentowany przez Wójta Gminy Miedzichowo Stanisława Piechotę.
- Administratorem Bezpieczeństwa Informacji/Inspektorem ochrony danych osobowych jest :

Marcin Cichowski
admin@miedzichowo.pl
Nr tel: 693641037

- dane osobowe są przetwarzane w związku ze złożoną ofertą dot. naboru na wolne stanowisko pracy,
- podstawą prawną do przetwarzania danych osobowych jest ustawa Kodeks Pracy (Dz.U. z 2018 r. poz. 108 t.j.)
- dane osobowe mogą być przekazywane podmiotom uprawnionym na mocy przepisów prawa ,
- dane osobowe będą przechowywane przez okres 14 dni w przypadku nie przyjęcia kandydata do pracy albo przez okres 10 lat po ustaniu zatrudnienia,
- osoba przekazująca swoje dane ma prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania ,
- osoba przekazująca swoje dane ma prawo do wniesienia sprzeciwu wobec przetwarzania a także prawo do przenoszenia danych osobowych,
- osoba przekazująca swoje dane ma prawo wniesienia skargi do GIODO/Urzędu Ochrony Danych Osobowych ,
- Podanie powyższych danych jest wymogiem ustawowym, brak lub podanie niepełnych danych może być podstawą do odrzucenia oferty,
- Urząd Gminy Miedzichowo nie przewiduje wykorzystania danych w celach innych niż w związku z naborem .

ANALIZA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI SYSTEMÓW INFORMATYCZNYCH POD KĄTEM ZAGROŻEŃ I RYZYKA

zwana dalej:

ANALIZĄ ZAGROŻEŃ I RYZYKA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Administrator Danych Osobowych: **Urząd Gminy Miedzichowo**

w osobie: **Stanisław Piechota**

dnia: **2018-01-02**

zgodnie z:

Art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, (Dz. U. z 2016r., poz. 922 z późn. zm.)
oraz
§ 4 pkt 5 ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004, nr 100, poz. 1024),

wprowadza dokument o nazwie:
„ANALIZA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI SYSTEMÓW INFORMATYCZNYCH POD KĄTEM ZAGROŻEŃ I RYZYKA"

zwanym dalej:
„ANALIZĄ ZAGROŻEŃ I RYZYKA PRZY PRZETWARZANIU DANYCH OSOBOWYCH"

Zapisy tego dokumentu wchodzą w życie z dniem ogłoszenia.

§ 1

Administrator Danych Osobowych ze względu na ciążące na nim obowiązki wynikające z ustawy o ochronie danych osobowych, a dokładnie art. 36 tej ustawy, zobowiązany jest do zastosowania środków technicznych i organizacyjnych, które mają zapewnić ochronę przetwarzanych danych osobowych, w świetle adekwatnych zagrożeń, 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.

§ 2

W związku z § 1 niniejszego dokumentu Administrator Danych Osobowych w osobie: **Stanisław Piechota** wprowadza dokument „Analiza zagrożeń i ryzyka" w celu badania i obserwowania istniejącego środowiska przetwarzania danych osobowych.

Ilekroć w „Analizie zagrożeń i ryzyka przy przetwarzaniu danych osobowych" jest mowa o:

1. **ANALIZIE RYZYKA** – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
2. **SZACOWANIU RYZYKA** – proces oceny i analizy ryzyka;
3. **OCENIE RYZYKA** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
4. **POSTĘPOWANIU Z RYZYKIEM** – wdrażanie środków modyfikujących ryzyko;
5. **ZARZĄDZANIU RYZYKIEM** – działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;
6. **RYZYKU SZCZĄTKOWYM** – ryzyko pozostające po procesie postępowania z ryzykiem;
7. **AKCEPTOWANIU RYZYKA** – decyzja, aby zaakceptować ryzyko;
8. **BEZPIECZEŃSTWIE INFORMACJI** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
9. **ZDARZENIU ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
10. **INCYDENCIE ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji;
11. **AKTYWACH** – wszystko, co ma wartość dla organizacji;
12. **ZAGROŻENIACH SYSTEMU** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
13. **DOSTĘPNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
14. **INCYDENCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO** — należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
15. **INFORMATYCZNYM NOŚNIKU DANYCH** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
16. **INTEGRALNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
17. **OPROGRAMOWANIU ZŁOŚLIWYM** — należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;
18. **PODATNOŚCI** — należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;
19. **POŁĄCZENIU MIĘDZYSYSTEMOWYM** — należy przez to rozumieć techniczne albo organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;
20. **POUFNOŚCI** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
21. **PRZEKAZYWANIU INFORMACJI** — należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;
22. **TESTACH BEZPIECZEŃSTWA** — należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym;
23. **ZABEZPIECZENIU** — należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;
24. **ZAGROŻENIU** — należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;
25. **ZASOBACH SYSTEMU TELEINFORMATYCZNEGO** – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

§ 4

Skuteczność zastosowanych środków powinna podlegać cyklicznym badaniom. Przy stosowaniu zabezpieczeń powinno się też uwzględniać zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany czy modernizowania wprowadzonych wcześniej przez Administratora Danych Osobowych systemów ochrony. Analiza zagrożeń i ryzyka, określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

§ 5

Wymogi ogólne bezpieczeństwa przetwarzanych danych osobowych, wprowadzone przez Administratora Danych Osobowych określa załącznik nr 1.

§ 6

Możliwe zagrożenia występujące w systemach informatycznych, określa załącznik nr 2.

§ 7

Podatność systemu na zagrożenia, określa załącznik nr 3.

§ 8

Analizę zagrożeń i ryzyka, określa załącznik nr 4.

§ 9

Wnioski i działania naprawcze, określa załącznik nr 5.

§ 10

Wzór klauzuli poufności, określa załącznik nr 6.

§ 11

Przebieg kontroli podatności systemu, określa załącznik nr 7.

§ 12

Rekomendacja odpowiedniej postawy upoważnionego do przetwarzania danych osobowych, określa załącznik nr 8.

§ 13

Tabela szacowania ryzyka została określona w załączniku nr 9.

WÓJT
dr Stanisław Piechota

.....

(Podpis Administratora Danych Osobowych)

WYMOGI OGÓLNE BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH, WPROWADZONE PRZEZ ADMINISTRATORA DANYCH OSOBOWYCH:

ADMINISTRATOR DANYCH OSOBOWYCH		IMIE I NAZWISKO
Urząd Gminy Miedzichowo	w osobie	Stanisław Piechota

§ 1

W czasie przetwarzania danych osobowych informacje mogą występować w postaci:

1. plików lub informacji przechowywanych na dysku twardym komputera;
2. plików lub informacji zapisanych na nośnikach komputerowych;
3. wersji roboczych lub gotowych dokumentów wydrukowanych na papierze.

§ 2

Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierające dane osobowe wymaga:

1. zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem;
2. ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem;
3. zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego;
4. zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników;
5. zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
6. zapewnienia możliwości kontroli nośników, na których przetwarzano lub przechowywano dane osobowe.

WÓJT
dr Stanisław Piechota
.....
(Podpis Administratora Danych Osobowych)

ZAGROŻENIA WYSTĘPUJĄCE W SYSTEMACH INFORMATYCZNYCH

§ 1

W myśl ustawy o ochronie danych osobowych, każdy Administrator Danych Osobowych powinien zapewnić takie warunki pracy w systemie, aby cechował się on poufnością, integralnością i rozliczalnością.

§ 2

Każde zauważone zagrożenie związane z poufnością, integralnością lub rozliczalnością, powinno być niezwłocznie zgłoszone Administratorowi Danych Osobowych bądź wyznaczonemu Administratorowi Bezpieczeństwa Informacji.

§ 3

1. Poufność, to zapewnienie danym osobowym niemożności ich udostępniania nieupoważnionym osobom czy podmiotom.
2. Zapewnienie poufności wartości informacyjnych wynika z obowiązku wypełnienia nakładanych na Administratora Danych Osobowych zadań, wynikających z ustaw, wraz z wszelkimi konsekwencjami organizacyjnymi i prawnymi.
3. Strategiczną częścią zabezpieczania danych w systemach informatycznych przed utratą poufności jest odpowiednio prowadzony system szkoleń dla pracowników merytorycznych mających dostęp do informacji.
4. Na Administratorze Bezpieczeństwa Informacji z ramienia ustawy spoczywa obowiązek zapoznania osób upoważnionych do przetwarzania danych z przepisami o ochronie danych osobowych oraz konsekwencjami prawnymi z nich wynikającymi.
5. Utrata poufności informacji o zasadach funkcjonowania systemów i sieci oraz mechanizmach zabezpieczeń jest niezwykle ważna oraz wymaga położenia nacisku na przestrzeganie procedur przez osoby sprawujące opiekę nad systemami i siecią.

§ 4

Zagrożenia, jakie można wyróżnić ze względu na utratę poufności w systemie informatycznym:

1. nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe;
2. ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe;
3. nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;
4. utrata nośnika zawierającego dane osobowe;
5. klęska żywiołowa, w wyniku której utracono poufność danych osobowych;

6. nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym;
7. udostępnianie danych osobowych osobom nieupoważnionym;
8. wejście w posiadanie danych osobowych przez osobę nieuprawnioną;
9. pokonanie zabezpieczeń fizycznych lub programowych;
10. niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych osobowych;
11. niedyskrecja osób uprawnionych do przetwarzania danych osobowych;
12. nieuprawnione kopiowanie danych na nośniki informacji (CD, DVD, pendrive, itp.);
13. niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych;
14. naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych;
15. podsłuch lub podgląd danych osobowych;
16. elektromagnetyczna emisja ujawniająca;
17. podsłuch akustyczny i podsłuch emisji ujawniającego promieniowania elektromagnetycznego;
18. stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy;
19. zagubienie dokumentów lub utrata przetwarzanych informacji.

§ 5

Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Brak skutków utraty poufności
< 1 – 3 >	Niski skutek utraty poufności
< 4 – 7 >	Średni skutek utraty poufności
< 8 – 9 >	Wysoki skutek utraty poufności
< 9 – 10 >	Całkowita utrata poufności

§ 6

1. Integralność to zapewnienie, aby wszelkie modyfikacje wykonywane w systemie informatycznym, w systemie jego katalogów oraz indywidualnych plikach posiadające w sobie dane osobowe były skutkiem rozważnych i zaplanowanych działań użytkowników systemu.
2. Integralność, to cecha zapewniająca, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieautoryzowany.
3. Integralność danych dotyczy przede wszystkim wartości informacyjnych przetwarzanych w postaci elektronicznej. Dlatego tak ważne jest zachowanie integralności dla bezpieczeństwa systemu i sieci.

4. Administrator Danych Osobowych powinien objąć procedurami weryfikacji i rozliczania pracowników sprawujących opiekę nad systemami i siecią oraz wprowadzić bieżącą, regularną detekcję prób ingerencji do systemu informatycznego oraz wszelkie próby naruszenia jego struktury, ponieważ skutkiem takich działań jest uszkodzenie bazy danych i w rezultacie naruszenie zapisów ustawy.

§ 7

Zagrożenia, jakie można wyróżnić ze względu na utratę integralności przez system informatyczny:

1. nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego;
2. błędy, pomyłki;
3. brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika;
4. wadliwe działanie systemu operacyjnego;
5. brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.
6. uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych;
7. celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
8. działanie złośliwego oprogramowania (wirusy);
9. pożar, zalanie, ekstremalna temperatura, itp.;
10. zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).

§ 8

Skala identyfikacji skutków utraty zasobów dla atrybutu integralności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata integralności nie występuje
< 1 – 3 >	Niski skutek utraty integralności
< 4 – 7 >	Średni skutek utraty integralności
< 8 – 9 >	Wysoki skutek utraty integralności
< 10 >	Bezwzględny skutek utraty integralności

§ 9

Rozliczalność to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu, jednemu podmiotowi.

§ 10

Zagrożenia, jakie można wyróżnić ze względu na utratę rozliczalności systemu informatycznego:

1. brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania;
2. wyparcie się pracy na stanowisku komputerowym, gdzie przetwarza się dane osobowe;
3. wprowadzenie zmian w treści dokumentu zawierającego dane osobowe;
4. błędy oprogramowania lub sprzętu;
5. nieprzydzielenie użytkownikom indywidualnych identyfikatorów;
6. niewłaściwa administracja systemem informatycznym;
7. niewłaściwa konfiguracja systemu informatycznego;
8. zniszczenie lub sfałszowanie logów systemowych;
9. brak rejestracji udostępnienia danych osobowych;
10. podszywanie się pod innego użytkownika;
11. niespełnienie przez system wymagań ustawowych.

§ 11

Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata rozliczalności nie występuje
< 1 – 3 >	Niski skutek utraty rozliczalności
< 4 – 6 >	Średni skutek utraty rozliczalności
< 7 – 8 >	Wysoki skutek utraty rozliczalności
< 9 >	Ekstremalny skutek utraty rozliczalności
< 10 >	Absolutny skutek utraty rozliczalności

§ 12

Dla systemów informatycznych szczególnie niebezpieczne są występujące zagrożenia stanowisk komputerowych, które występują przeważnie ze względu na ingerencję:

1. **SIŁY NATURY** (to zdarzenia niewynikające z działalności człowieka), mogą to być:
   a) uderzenie pioruna;
   b) pożar będący konsekwencją ww. uderzenia pioruna;
   c) starzenie się sprzętu;
   d) starzenie się nośników pamięci;
   e) smog, kurz;

f) katastrofy budowlane;
g) ulewny deszcz;
h) huragan;
i) ekstremalne temperatury, wilgotność;
j) epidemia.

2. **LUDZI** (mogą to być pracownicy lub osoby z zewnątrz, które działają w sposób celowy lub przypadkowy), mogą to być:

a) błędy i pomyłki użytkowników;
b) błędy i pomyłki administratorów;
c) błędy utrzymania systemu w poufności, integralności i rozliczalności;
d) zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu;
e) zagubienie nośnika zawierającego dane osobowe;
f) niewłaściwe zniszczenie nośnika;
g) nielegalne użycie oprogramowania;
h) choroba ważnych osób i nieuprawnione zastępstwo;
i) epidemia kadry i brak osób upoważnionych do dostępu;
j) podpalenie obiektu;
k) zalanie wodą;
l) katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka;
m) zakłócenia elektromagnetyczne, radiotechniczne;
n) podłożenie i wybuch bomby, ładunku wybuchowego;
o) użycie broni;
p) zmiany napięcia w sieci;
q) utrata prądu;
r) zbieranie się ładunków elektrostatycznych;
s) utrata kluczowych pracowników;
t) niedobór pracowników;
u) defekty oprogramowania;
v) szpiegostwo;
w) terroryzm;
x) wandalizm;
y) destrukcja zbiorów i programów impulsem elektromagnetycznym;
z) kradzież;
aa) włamanie do systemu;
bb) wyłudzenie, fałszowanie dokumentów;
cc) podszycie się pod uprawnionego użytkownika;
dd) podsłuch;
ee) użycie złośliwego oprogramowania;
ff) wykorzystanie promieniowania ujawniającego.

WÓJT
dr Stanisław Piechota

.....

(Podpis Administratora Danych Osobowych)

PODATNOŚĆ SYSTEMU NA ZAGROŻENIA

§ 1

Podatność systemu na zagrożenia stanowi pewnego rodzaju słabość. Obecnie, szczególnie trudno jest obronić się przed zagrożeniami w zakresie teleinformatycznym, co związane jest z coraz to bardziej wyrafinowaną cyberprzestępczością. Wraz z coraz to większą ilością dostępnych w środowisku internetowym usług, nasilają się działania przestępcze. Chroniąc placówkę przed takowym działaniem, należy wdrożyć odpowiednie procedury.

§ 2

Podatność systemu na zagrożenia może wynikać z:

1. **Dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę, jak obsługiwać system.**

   Fizyczna ochrona danych osobowych to jeden z podstawowych obszarów w zakresie przetwarzania danych osobowych. Osoba przetwarzająca dane osobowe bardzo często nie zdaje sobie sprawy, jak ważne jest przestrzeganie chociażby „zasady czystego biurka", która bardzo często jest marginalizowana i zwyczajnie nieprzestrzegana. Bardzo często nieświadomość pracowników w tej materii wiąże się z negatywnymi konsekwencjami dla placówki, np. kwestia złożenia skargi, której przedmiotem jest niedochowywanie należytej staranności w zakresie fizycznej ochrony danych osobowych. Proces wdrażania w placówce „kodeksu dobrych praktyk" w kontekście ochrony danych osobowych jest procesem długoletnim i dynamicznym, ale bezsprzecznie powinno się w pierwszej kolejności uwrażliwiać na fizyczną ochronę danych osobowych. Ponadto, tylko i wyłącznie osoby upoważnione do przetwarzania danych osobowych powinny posiadać wiedzę o tym, w jaki sposób obsługiwać system informatyczny, będący integralnym elementem placówki.

2. **Dostępności informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych.**

   System informatyczny w placówce powinien być odpowiednio zabezpieczony, również jeśli dostęp do niego jest możliwy za pośrednictwem połączeń zewnętrznych. Niezależnie od zastosowanych rozwiązań teletransmisyjnych, system ten powinien być „szczelny", to znaczy wystarczająco odporny na wszelkiego rodzaju zewnętrzne zagrożenia.

3. **Możliwości celowego wprowadzania luk w sprzęcie i oprogramowaniu lub wprowadzania wirusów komputerowych.**

   Możność nieuprawnionego działania na sprzęcie, czy oprogramowaniu może być wynikiem zastosowanej manipulacji, podsłuchu czy podstawienia. Podsłuch polega na tym, że charakter poufności przekazywanych treści zostaje naruszony. Manipulacja z kolei, będzie działaniem, które ukierunkowane jest na uzyskanie dostępu do treści danych i nieuprawnioną ingerencję w nie. Natomiast podstawienie, polega między innymi na wprowadzeniu drugiej strony w błąd, co do swojej tożsamości, po to tylko, by uzyskać konkretne informacje. Kadra powinna być odpowiednio uwrażliwiona na otrzymywanie korespondencji mailowej, co do której zaistnieje podejrzenie, że została przesłana w celu wprowadzenia wirusa komputerowego.

4. **Możliwości awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję.**

   Sprzęt informatyczny powinien być cyklicznie odpowiednio serwisowany, tak by wyeliminować zagrożenia. Należy zaznaczyć, iż z firmą informatyczną zewnętrzną, nie podpisujemy upoważnienia do przetwarzania danych osobowych, ale przynajmniej klauzulę poufności informacji w kontekście przetwarzanych danych osobowych. Wzór klauzuli poufności stanowi załącznik nr 7.

5. **Przesyłania informacji przez niezabezpieczone łącza telekomunikacyjne.**

   Brak zabezpieczeń kryptograficznych łącza telekomunikacyjnego czy nieefektywność fizycznych zabezpieczeń, również stanowi zagrożenie utraty poufności danych osobowych.

§ 3

1. Podatność systemu na zagrożenia została ograniczona poprzez:
   a) ochronę fizyczną stanowisk komputerowych;
   b) kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe;
   c) wydzielenie stref ochronnych;
   d) ograniczenie liczby personelu, mającego potencjalnie dostęp do stanowisk komputerowych oraz wiedzę, jak je obsługiwać;
   e) zbudowanie stabilnej sieci zasilającej;
   f) przeglądy okresowe nośników;
   g) kontrolę zmian konfiguracji;
   h) testowanie oprogramowania;
   i) audyt;
   j) zabezpieczanie haseł;
   k) użycie oprogramowania antywirusowego;
   l) backupy.
2. By maksymalnie wyeliminować zagrożenie dla całego systemu ochrony danych osobowych, należy wdrożyć procedury kontrolne, które nie będą zorientowane tylko i wyłącznie na jeden obszar przetwarzania danych osobowych, tj. środowisko komputerowe. Warunkiem wyeliminowania działań cyberprzestępców, jest pełne współdziałanie wszystkich obszarów przetwarzania danych osobowych:
   a) prowadzenie odpowiedniej dokumentacji;
   b) fizyczna ochrona danych osobowych;
   c) środowisko komputerowe;
   d) „kodeks dobrych praktyk" wdrożony przez Administratora Bezpieczeństwa Informacji, o ile jest powołany lub Administratora Danych Osobowych.
3. Przebieg przykładowej kontroli tych obszarów stanowi załącznik nr 8.

§ 4

W celu wdrażania systemu ochrony danych osobowych w taki sposób, by uniemożliwić działanie nieuprawnione na danych osobowych, Administrator Danych Osobowych zobowiązuje pracowników podmiotu o nazwie: **Urząd Gminy Miedzichowo** do stosownego zachowania w trakcie przetwarzania danych osobowych, czego aprobatę wyraził w swojej rekomendacji, która stanowi załącznik nr 9.

§ 5

W celu oszacowania potencjalnych strat wynikających z utraty (ujawnienia) danych osobowych przetwarzanych na stanowiskach komputerowych, wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów. Analiza ryzyka musi być wykonywana okresowo przez Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego - raz do roku na tej podstawie aktualizowana jest tabela ryzyka znajdująca poniżej - § 6.

§ 6

Identyfikacja podatności systemu informatycznego na określone zagrożenia.

WARTOŚĆ	SKUTKI
< 0 >	Brak podatności
< 1 – 4 >	Niski poziom
< 5 – 7 >	Średni poziom
< 8 – 9 >	Wysoki poziom
< 10 >	Ekstremalny poziom

WÓJT
Stanisław Piechota
.....
(Podpis Administratora Danych Osobowych)

ANALIZA ZAGROŻEŃ I SZACOWANIE RYZYKA

§ 1

Administrator Danych Osobowych, aby poprawnie przeprowadzić analizę ryzyka, powinien określić:

1. **ZASOBY** - które będzie chronić:
   a) sprzęt komputerowy przechowujący dane - dysk twardy,
   b) dane osobowe przetwarzane w formie papierowej i elektronicznej,
   c) aplikacje, w których przetwarzane są dane osobowe,
   d) pomieszczenia, w których pracują osoby przetwarzające dane osobowe;
2. **ZAGROŻENIA** - czynnik, który może powodować wystąpienie incydentu;
3. **PODATNOŚĆ** - słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie;
4. **SKUTKI** - jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.

§ 2

Administrator Danych Osobowych bądź Administrator Bezpieczeństwa Informacji, aby dokonać skutecznego zarządzania bezpieczeństwem informacji w podmiocie, dokonuje dokładnej analizy zagrożeń w związku z reagowaniem na zmieniające się warunki otoczenia mające wpływ na ryzyko w organizacji. Tak stworzony efektywny system zarządzania daje możliwość podjęcia działań redukujących wartość ryzyka do akceptowanego poziomu.

§ 3

Poniższy schemat obrazuje prawidłowy tok szacowania i postępowania z ryzykiem, jakie podejmuje Administrator Danych Osobowych.

§ 4

1. Analiza ryzyka jest częścią szacowania ryzyka. Jest ona pojęciem węższym niż szacowanie ryzyka, nie zawiera bowiem oceny ryzyka.
2. Ocena ryzyka, czyli określenie, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyka z tymi, które można zaakceptować.
3. Szacowanie ryzyka obejmuje analizę ryzyka i ocenę ryzyka.

§ 5

1. Administrator Danych Osobowych szacuje wynik ryzyka. Poprzez określenie poziomu ryzyka akceptowalnego i kończy etap szacowania ryzyka.
2. Administrator Danych Osobowych wyciąga wnioski oraz podejmuje działania naprawcze, mające na celu obniżenie wartości ryzyka akceptowalnego.
3. Tabela szacowania ryzyka stanowi załącznik nr 9.

§ 6

1. Administrator Danych Osobowych określa poziom ryzyka utraty bezpieczeństwa danych osobowych na poziomie **NISKI** w podmiocie o nazwie **Urząd Gminy Miedzichowo** przy uwzględnieniu ryzyka ogólnego przy wartości 8,64.

   RYZYKO = wartość skutków x podatność zasobów systemu

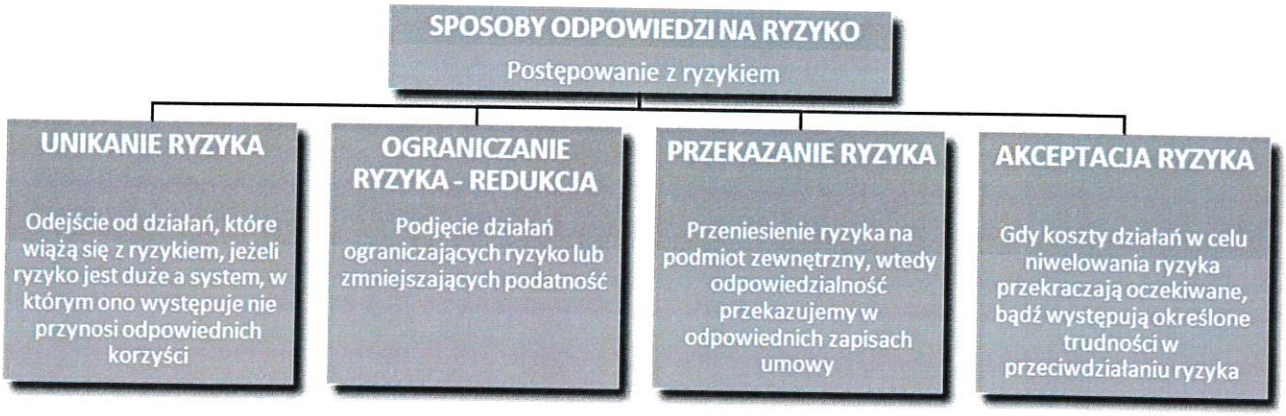
   (max. = 100)

WARTOŚĆ	POZIOM RYZYKA
<1-20>	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<21-60>	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<61-80>	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<81-100>	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

2. Poziomy ryzyka utraty bezpieczeństwa danych osobowych:
   a) **NISKI** – niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia;
   b) **ŚREDNI** – wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji;
   c) **WYSOKI** – wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia;
   d) **MAKSYMALNY** – wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

§ 7

Administrator Danych Osobowych po oszacowaniu ryzyka przystępuje do etapu postępowania z ryzykiem. Koniecznym jest podjęcie działania, które będzie odpowiedzią podmiotu na oszacowany poziom występującego ryzyka. W ramach postępowania z ryzykiem możemy podjąć cztery różne działania.



§ 8

Proces zarządzania ryzykiem związany z bezpieczeństwem informacji zapewnia:

1. identyfikowanie zagrożeń dla przetwarzanych informacji;
2. oszacowanie ryzyka w kategoriach konsekwencji dla funkcjonowania biznesowego oraz prawdopodobieństwa wystąpienia zagrożeń;
3. odpowiednie przedstawienie oraz zrozumienie prawdopodobieństwa oraz konsekwencji materializacji ryzyka;
4. ustanowienie priorytetów dotyczących postępowania z ryzykiem;
5. wprowadzanie priorytetowych działań mających na celu redukcję ryzyka;
6. zaangażowanie kierownictwa podczas podejmowania decyzji związanych z zarządzaniem ryzykiem oraz bieżące informowanie go o postępach realizowanych działań minimalizujących;
7. monitorowanie i regularne przeglądanie ryzyka oraz procesu zarządzania nimi;
8. kształcenie pracowników w zakresie ryzyka oraz działań mających na celu obniżenie poziomu prawdopodobieństwa ich wystąpienia.

WÓJT
dr Stanisław Piechota
.....
(Podpis Administratora Danych Osobowych)

WNIOSKI I DZIAŁANIA NAPRAWCZE W ZWIĄZKU Z PRZEPROWADZONĄ „ANALIZĄ RYZYKA I ZAGROŻEŃ PRZY PRZETWARZANIU DANYCH OSOBOWYCH"

§ 1

1. Administrator Danych Osobowych w osobie: **Stanisław Piechota** przeprowadził analizę dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń.
2. Administrator Danych Osobowych jest zobowiązany dostosować środki bezpieczeństwa, zarówno techniczne, jak i fizyczne oraz organizacyjne, do wyników, jakie oddała przeprowadzona analiza.
3. Zmiany związane z pkt 2 należy wprowadzić do aktualnej Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

§ 2

W wyniku przeprowadzonej analizy w placówce o nazwie: **Urząd Gminy Miedzichowo** Administrator Danych Osobowych wyróżnił potencjalnie najniebezpieczniejsze zagrożenia, a w szczególności są to:

- Ataki wirusów w tym ransomware na aplikacje ,
- Nieuprawniony dostęp do pomieszczeń w których przetwarza się dane osobowe ,
- Ryzyko kradzieży danych osobowych.

§ 3

W celu zmniejszenia zagrożeń, wymienionych w § 2 przez Administratora Danych Osobowych, należy zwrócić uwagę w szczególności na:

- Regularną aktualizację ochrony antywirusowej, ,
- Cykliczne dokształcania oraz podnoszenie świadomości pracowników w zakresie ochrony d.o.,
- Zwiększenie nakładów na infrastrukturę IT.

§ 4

Administrator Danych Osobowych w celu wyeliminowania zagrożeń, wynikłych w toku przeprowadzonej analizy, podejmuje działania naprawcze, polegające w szczególności na:

- ..... ,
- ..... ,
- ..... .

WÓJT
dr Stanisław Piechota
.....
(Podpis Administratora Danych Osobowych)

WZÓR KLAUZULI POUFNOŚCI INFORMACJI [1]

§ 1

Strony umowy zobowiązują się wzajemnie do niewykorzystywania, nieujawniania oraz nieprzekazywania informacji, które stanowią tajemnicę przedsiębiorstwa drugiej strony niniejszej umowy.

§ 2

Strony powinny zachować poufność informacji, które zdobędą na każdym etapie jakiejkolwiek wzajemnej współpracy.

§ 3

Klauzula poufności danych obowiązuje strony przez okres trwania umowy, a także bezwzględnie po jej zakończeniu przez okres ..... lat.

§ 4

Strony odpowiadają za zachowanie powyższych informacji w tajemnicy przez osoby, którym wykonanie swoich obowiązków powierzyły.

§ 5

Strony umowy zobowiązują się do wykorzystywania przetwarzanych przez nie danych osobowych, w ramach realizacji niniejszej umowy, wyłącznie w celach określonych w umowie.

§ 6

Stronom umowy przysługuje w każdym czasie i bez ograniczenia - kontrola procesu przetwarzania i ochrony danych osobowych.

§ 7

Strony, dopełniając czynności wynikających z niniejszej umowy, zobowiązują się do przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016r., poz. 922 z późn. zm.).

§ 8

W przypadku niedochowania warunków umowy, strony zastrzegają sobie prawo rozwiązania niniejszej umowy w trybie natychmiastowym, w każdym czasie.

[1] **UWAGA:** Ninlejszy dokument może być zastosowany:

- jako osobny (niezależny) dokument celem zobowiązania drugiej strony do zachowania poufności informacji,
- jako dodatkowe zapisy (paragrafy) do umowy lub innego dokumentu wiążącego strony wzajemną współpracą.

PRZEBIEG KONTROLI PODATNOŚCI SYSTEMU

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
1.	DOKUMENTACJA	Sprawdzenie, czy Polityka Bezpieczeństwa oraz Instrukcja Zarządzania Systemem Informatycznym jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.
2.	DOKUMENTACJA	Sprawdzenie, czy osoba ma upoważnienie do przetwarzania danych osobowych – upoważnienie powinno odzwierciedlać zakres obowiązków.
3.	DOKUMENTACJA	Sprawdzenie, czy osoby, które mają dostęp do danych osobowych, ale nie przetwarzają tych danych, posiadają zgody na przebywanie w obszarze przetwarzania.
4.	DOKUMENTACJA	Sprawdzenie, czy prowadzona jest aktualna ewidencja osób przetwarzających dane osobowe.
5.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Kontrolowanie osób przetwarzających dane osobowe - czy stosują się do „zasady czystego biurka".
6.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie (jeśli tak - można sporządzić dokumentację fotograficzną pomieszczeń, która stanowić będzie załącznik do poniższego sprawdzenia).
7.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajduje się niszczarka dokumentów (jeśli takie urządzanie nie znajduje się w pomieszczeniu, należy skontrolować pracownika, w jaki sposób niszczy zbędną dokumentację, która nie podlega archiwizacji). Szczególnie powinno się zwrócić uwagę, czy niepotrzebne dokumenty nie są przypadkiem wyrzucane do kosza na śmieci – dokumenty powinny być niszczone w sposób mechaniczny lub manualny, tak, by uniemożliwić ich odczytanie osobom postronnym.
8.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, mające na celu sprawdzenie, czy komputer jest zabezpieczony hasłem.
9.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy systemy komputerowe służące do przetwarzania danych osobowych zapamiętują wszelakie czynności, jakich dokonuje się przy przetwarzaniu danych osobowych.
10.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Monitorowanie, czy osoby przetwarzające dane osobowe w programie komputerowym bazodanowym (czyli dotyczącym baz danych) logują się za pomocą WŁASNEGO identyfikatora i hasła.
11.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie aktywności systemu antywirusowego, na komputerach, które m.in. służą do obsługi systemów przetwarzających dane osobowe.
12.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
13.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych - osobom postronnym.
14.	ZBIORY DANYCH OSOBOWYCH	Kontrolowanie, czy wszystkie zbiory danych osobowych, które podlegają obowiązkowej rejestracji w GIODO, zostały prawidłowo zgłoszone.
15.	ZBIORY DANYCH OSOBOWYCH	Sprawdzenie, czy wszystkie zbiory, które prowadzi się w placówce, a podlegają wpisowi do jawnego rejestru, zostały w owym dokumencie wpisane i odpowiednio ogłoszone do publicznej wiadomości (np. za pośrednictwem Biuletynu Informacji Publicznej).
16.	ZBIORY DANYCH OSOBOWYCH	Przeprowadzenie wywiadu, którego celem jest ustalenie, czy pracownik przetwarza zbiór danych osobowych, który nie został zgłoszony do tej pory do GIODO (szczególnie ma się na względzie projekty prowadzone przez referaty).
17.	KONTROLA PRAKTYKI	Przeprowadzenie analizy pod kątem pracowników - jakie obecnie mają problemy w zakresie przetwarzania danych osobowych oraz czy ostatnio miały miejsce zdarzenia typu: • próby nieuprawnionego dostępu do danych osobowych; • działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania; • nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym; • próba nieuprawnionej interwencji przy sprzęcie komputerowym; • wynoszenie niezabezpieczonych pamięci z miejsca pracy; • udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny.

REKOMENDACJA ODPOWIEDNIEJ POSTAWY OSÓB POSIADAJĄCYCH UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

Przepisy kodeksu pracy zobowiązują pracownika do sumiennego wykonywania swoich obowiązków. Pracownik powinien odpowiednio przestrzegać czasu pracy, co w konsekwencji oznacza, że nie powinien on w godzinach pracy zajmować się prywatnymi sprawami, chociażby prywatną korespondencją.

§ 2

Pracodawca wyposaża pracowników w konkretne narzędzia pracy, jak telefon czy komputer i nie musi godzić się na wykorzystywanie ich do prywatnych celów.

§ 3

Pracodawca może kontrolować pracownika w ramach stosownego wykorzystywania narzędzi, które powinny służyć tylko do celów służbowych. Za interesem pracodawcy przemawia fakt, że musi on chronić tajemnicę przedsiębiorstwa oraz zabezpieczać odpowiednio placówkę pod względem systemu ochrony danych osobowych.

§ 4

Należy przypomnieć niniejszym dokumentem, iż w placówce wdrożono postanowienia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym, co w konsekwencji oznacza, iż dobrych praktyk powinno się przestrzegać.

§ 5

Jeśli pracodawca podczas kontroli stwierdzi, iż zakaz nie jest respektowany, może wobec pracownika wyciągnąć konsekwencje służbowe.

§ 6

Pracodawca może ustalić, że na służbowych komputerach nie można instalować aplikacji oraz używania portali społecznościowych. Ponadto, pracodawca może zakazać wnoszenia prywatnych nośników danych tj. nośników: optycznych (płyty CD, DVD itp.), półprzewodnikowych (układy scalone), magnetycznych (w tym pamięci ferrytowe), magnetooptycznych, polimerowych (np. Millipede), papierowych (np. karty dziurkowane), z linią opóźniającą (np. pamięci rtęciowe).

§ 7

Pracodawca niniejszym dokumentem informuje pracowników, iż kontrola w danym zakresie będzie miała miejsce, a pracownicy przyjmują ten fakt do wiadomości.

§ 8

Powyższe wskazania mają swoje uzasadnienie w interpretacji Generalnego Inspektora Danych Osobowych (serwis prawno-pracowniczy nr 39/2012 s. 7-8; link: http://spp.infor.pl/).

WÓJT
dr Stanisław Piechota

.....

(Podpis Administratora Danych Osobowych)

TABELA SZACOWANIA RYZYKA

00SZACOWANIE RYZYKA DLA BEZPIECZEŃSTWA INFORMACJI																	RYZYKO OGÓLNE [3] :
		RYZYKO ŚREDNIE [2] :			9,27			7,22			12,17			5,89	8,64		
	OZAGROŻENIA0	INTEGRALNOŚĆ	AWARIA SPRZĘTU	5	3	15	0	0	0	0	0	0	0	0	0		
			ODCIĘCIE ZASILANIA	1	4	4	0	0	0	5	2	10	0	0	0		
			POŻAR	1	2	2	5	2	10	1	1	1	5	2	10		
			ATAK WIRUSA	0	0	0	0	0	0	5	8	40	0	0	0		
			KRADZIEŻ	2	4	8	5	5	25	5	1	5	0	0	0		
			NIEUPRAWNIONY DOSTĘP	5	4	20	5	3	15	8	2	16	5	5	25		
		ROZLICZALNOŚĆ	AWARIA SPRZĘTU	5	3	15	0	0	0	0	0	0	0	0	0		
			ODCIĘCIE ZASILANIA	1	4	4	0	0	0	0	0	0	0	0	0		
			POŻAR	1	2	2	5	2	10	1	1	1	5	2	10		
			ATAK WIRUSA	0	0	0	0	0	0	8	5	40	0	0	0		
			KRADZIEŻ	2	4	8	3	5	15	5	1	5	0	0	0		
			NIEUPRAWNIONY DOSTĘP	5	4	20	4	3	15	8	5	40	5	5	25		
		POUFNOŚĆ	AWARIA SPRZĘTU	5	3	15	0	0	0	0	0	0	0	0	0		
			ODCIĘCIE ZASILANIA	1	4	4	0	0	0	0	0	0	1	1	1		
			POŻAR	5	2	10	5	2	10	0	0	0	5	2	10		
			ATAK WIRUSA	0	0	0	0	0	0	8	5	40	0	0	0		
			KRADZIEŻ	5	4	20	5	5	25	2	1	5	0	0	0		
			NIEUPRAWNIONY DOSTĘP	5	4	20	5	3	15	8	2	16	5	5	25		
		SZACOWANIE		SKUTKI	PODATNOŚĆ	RYZYKO [4]	SKUTKI	PODATNOŚĆ	RYZYKO [4]	SKUTKI	PODATNOŚĆ	RYZYKO [4]	SKUTKI	PODATNOŚĆ	RYZYKO [4]		
		ZASOBY SZACOWANE		SPRZĘT			D.O. W FORMIE PAPIEROWEJ			APLIKACJA			POMIESZCZENIA				

Skala poziomu ryzyka:

[2] **RYZYKO ŚREDNIE** = suma ryzyka każdego z sześciu zakresów poufności, rozliczalności i integralności dzielona przez 18

[3] **RYZYKO OGÓLNE** = suma ryzyka średniego z zasobów: sprzęt, ludzie, aplikacja, pomieszczenia, zabezpieczenia dodatkowe, dzielona przez 4

[4] **RYZYKO** = wartość skutków x podatność zasobów systemu (max. = 100)

WARTOŚĆ	POZIOM RYZYKA
1-20	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
21-60	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
61-80	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
81-100	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

PODSUMOWANIE

W podmiocie o nazwie: **Urząd Gminy Miedzichowo** po przeprowadzeniu analizy poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka, zwanej dalej: analizą zagrożeń i ryzyka przy przetwarzaniu danych osobowych wartość i poziom ryzyka przedstawia się następująco:

Ryzyko ogólne wynosi: **8,64**

Powyższa wartość ryzyka określa **NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych.

WÓJT
dr Stanisław Piechota

.....

(Data i Podpis Administratora Danych Osobowych)

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych Osobowych – **Urząd Gminy Miedzichowo**
w osobie: **Stanisław Piechota** dnia **02-01-2018 r.**

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 02-01-2018 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 2016r. poz. 922 z późn. zm.), 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 2016r., poz. 1489 z późn. zm.),
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.

§ 1

W podmiocie o nazwie: **Urząd Gminy Miedzichowo** za przestrzeganie zapisów „instrukcji" odpowiedzialny jest **Administrator Danych** lub zgodnie z zapisem §3 „Polityki Bezpieczeństwa" wyznaczony **Administrator Bezpieczeństwa Informacji.**

§ 2

W związku z tym, że w podmiocie o nazwie: **Urząd Gminy Miedzichowo** 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 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: **Norton Security Premium**,
   - 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: **Biuro nr 4**, 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:

   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 Bezpieczeństwa Informacji, o ile jest wyznaczony, 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.**

Administrator Danych Osobowych

WÓJT
dr Stanisław Piechota

.....

Podpis

Administrator Bezpieczeństwa Informacji

.....

Podpis

ZATWIERDZAM

WÓJT
dr Stanisław Piechota

.....
Administrator Danych Osobowych

PLAN SPRAWDZENIA PLANOWEGO

dla

Administrator Danych Osobowych: **Urząd Gminy Miedzichowo**

w osobie: **Stanisław Piechota**

dnia: **2018-01-02**

sporządzony zgodnie z art.36 a ust.2 pkt 1 lit. a ustawy o ochronie danych osobowych oraz rozporządzenia Ministra Administracji i Cyfryzacji z dnia 29 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych.

Sprawdzenia dokona Administrator Bezpieczeństwa Informacji w **Urząd Gminy Miedzichowo** w terminie od dnia **10 stycznia 2018** do dnia **31 marca 2018**

1. Celem sprawdzenia planowego w ramach nadzoru jest ocena prawidłowości opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, także przestrzegania zasad określonych w powyższej dokumentacji.

2. Realizacja sprawdzenia planowego zostanie przeprowadzona w oparciu o weryfikację :
   1) opracowania i kompletności dokumentacji przetwarzania danych osobowych ;
   2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
   3) stanu faktycznego w zakresie przetwarzania danych osobowych;
   4) skuteczności przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych zabezpieczenia rozwiązań dla przeciwdziałania zagrożeniom dla ochrony danych osobowych;
   5) przestrzegania obowiązków określonych w dokumentacji przetwarzania danych osobowych.

3. W trakcie sprawdzenia zostanie dokonana inwentaryzacja zbiorów danych osobowych przetwarzanych przez administratora danych poprzez weryfikację zgodności przetwarzania danych osobowych :
   1) z zasadami, o których mowa w art.23-27 i art.31-35 ustawy;
   2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36 oraz art.37-39 ustawy;
   3) z zasadami przekazywania danych osobowych, o których mowa w art.47-48 ustawy;
   4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art.27 ust.1 ustawy.

PROGRAM SPRAWDZENIA I UPRAWNIENIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI
W RAMACH REALIZACJI PROGRAMU :

1. Sprawdzeniu będą podlegały następujące komórki organizacyjne i stanowiska pracy:

   1) Referat Księgowości od dnia 10.01.2018 do dnia 31.01.2018
      Obejmujący stanowiska:
      - Stanowisko ds. windykacji podatkowej, podatków od środków transportowych
      - Stanowisko ds. podatków i opłat
      - Główna Księgowa
      - Stanowisko ds. płac
      - Stanowisko ds. księgowości budżetowej gminy
      - Skarbnik Gminy

   2) Referat Spraw obywatelskich od dnia 01.02.2018 do dnia 14.02.2018
      Obejmujący stanowiska:
      - Stanowisko ds. pomocy rodzinie
      - Stanowisko ds. świadczeń wychowawczych oraz fundusz alimentacyjny
      - Kierownik USC, Kierownik Referatu Spraw Obywatelskich

   3) Referat Organizacyjny od dnia 15.02.2018 do dnia 28.02.2018
      Obejmujący stanowiska:
      - Stanowisko obsługi sekretariatu
      - Stanowisko ds. promocji gminy i kancelarii ogólnej
      - Stanowisko ds. obsługi organów gminy, ewidencja działalności gospodarczej, kadry
      - Sekretarz Gminy

   4) Referat Infrastruktury i Ochrony Środowiska od dnia 01.03.2018 do dnia 15.03.2018
      Obejmujący Stanowiska:
      - Stanowisko ds. dróg publicznych i zamówień publicznych i inwestycji komunalnych
      - Stanowisko ds. gospodarki gruntami i gospodarki, mieniem gminnym, gospodarowanie mieszkaniowym zasobem gminy
      - Stanowisko ds. gospodarki przestrzennej gminy
      - Stanowisko ds. pozyskiwania środków unijnych
      - Kierownik Referatu Infrastruktury i Ochrony Środowiska

   5) Referat Samodzielne stanowisko od dnia 16.03.2018 do dnia 25.03.2018
      Ds. wojskowych i obronnych, obrony cywilnej i ochrony przeciwpożarowej

   6) Stanowisko Wójta Gminy Miedzichowo od dnia 26.03.2018 do dnia 31.03.2018

2. W ramach planu sprawdzenia oraz realizacji programu, sprawdzenia i podejmowane działania uwzględniają uprawnienia administratora bezpieczeństwa do następujących czynności:
   1) zbieranie ustnych lub pisemnych wyjaśnień od osób objętych sprawdzeniem;

2) przeprowadzanie oględzin miejsc przetwarzania danych osobowych, a także uzyskiwanie dostępu do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
3) analizowanie dokumentów dotyczących przetwarzania danych osobowych przetwarzania danych osobowych.

3. Dokumentowanie czynności w ramach sprawdzeń urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych może być dokonane poprzez sporządzenie:
   1) notatki z czynności;
   2) protokołu odebrania ustnych wyjaśnień,
   3) protokołu z oględzin,
   4) kopii otrzymanego dokumentu;
   5) kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania danych osobowych;
   6) kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

Informacje dodatkowe:

1. Dokumentowanie czynności, których mowa w pkt.3 sporządzane mogą być w postaci papierowej albo w postaci elektronicznej,
2. W przypadku potrzeby administrator bezpieczeństwa informacji, po uzgodnieniu z administratorem danych może wystąpić o wydanie opinii przez osobę posiadająca wiedzę specjalistyczną nie dotyczącą przepisów o ochronie danych osobowych, niezbędną do zapewnienia prawidłowego przeprowadzenia sprawdzenia,
3. W systemie informatycznym służącym do przetwarzania danych osobowych czynności związane z oględzinami urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych są wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, w szczególności administratora systemu.
4. W przypadku wykrycia podczas weryfikacji nieprawidłowości administrator bezpieczeństwa informacji :
   1) zawiadamia administratora danych o nieopracowaniu lub brakach w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia do wymaganego stanu, w szczególności przedstawia mu do wdrożenia dokumenty usuwające stan niezgodności;
   2) zawiadamia administratora danych o nieaktualności dokumentacji przetwarzania danych oraz przedstawia administratorowi danych do wdrożenia dokumenty aktualizujące;
   3) poucza lub instruuje osoby nieprzestrzegające zasad określonych w dokumentacji przetwarzania danych osobowych o prawidłowym sposobie ich realizacji lub zawiadamia administratora danych, wskazując osoby odpowiedzialne za naruszenie tych zasad i ich zakres.
5. Sprawozdanie ze sprawdzenia planowego dla administratora danych zostanie przekazane w terminie określonym w planie sprawdzeń, nie później niż w terminie 30 dni od dnia zakończenia sprawdzenia,
6. Plan jest przedstawiany administratorowi danych nie później niż na 14 dni przed rozpoczęciem okresu objętego planem,

7. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

OPRACOWAŁ
Administrator Bezpieczeństwa Informacji
Marcin Cichowski