Załącznik Nr 1
do Zarządzenia Nr 102/2016
Wójta Gminy Wydminy
z dnia 6 grudnia 2016 roku

Polityka bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych w Urzędzie Gminy Wydminy

I -Część ogólna

§ 1. Realizując postanowienia ustawy o ochronie danych osobowych (t. j. Dz. U. z 2016r. poz. 922) oraz wydane w oparciu o delegację ustawową przepisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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), Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r. poz. 719 ze zm.) i Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r. poz. 745 ze zm.), ustanawia się „Politykę bezpieczeństwa danych osobowych i danych wrażliwych w Urzędzie Gminy Wydminy” , zwaną dalej „Polityką bezpieczeństwa”.

§ 2. Ilekroć w niniejszym dokumencie jest mowa o:

1. Urzędzie - należy przez to rozumieć Urząd Gminy Wydminy,
2. Ustawie - należy przez to rozumieć ustawę o ochronie danych osobowych, o której mowa w § 1 niniejszej części,
3. ADO - należy przez to rozumieć Administratora Danych Osobowych w rozumieniu ustawy, Administratorem Danych jest Wójt Gminy Wydminy. W imieniu Administratora Danych obowiązki określone w Ustawie pełni Administrator Bezpieczeństwa Informacji,
4. ABI - należy przez to rozumieć Administratora Bezpieczeństwa Informacji w rozumieniu ustawy,
5. ASI - należy przez to rozumieć Administratora Systemów Informacyjnych,
6. Polityce – należy przez to rozumieć „Politykę bezpieczeństwa”, obowiązującą w Urzędzie Gminy Wydminy,
7. Instrukcji – należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy Wydminy,
8. GIODO - należy przez to rozumieć Generalnego Inspektora Ochrony Danych Osobowych,
9. Sprawdzeniu - należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzanych osobowych z przepisami o ochronie danych osobowych,
10. Sprawozdaniu - należy przez to rozumieć dokument, o którym mowa w art. 36c ustawy, opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia,
11. Użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w Urzędzie, osoba wykonująca pracę na podstawie umowy – zlecenia lub innej umowy cywilno - prawnej, osoba odbywająca staż w Urzędzie,
12. Systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych,

13. Przetwarzaniu danych – należy przez to rozumieć jakiekolwiek operacje, wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
14. Zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
15. Danych osobowych – danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności, np. sama nazwa ulicy i numer domu, w którym mieszka wiele osób. Informacja ta będzie jednak stanowić dane osobowe wówczas, gdy zostanie zestawiona z innymi, dodatkowymi informacjami, np. imieniem i nazwiskiem czy numerem PESEL, które w konsekwencji można odnieść do konkretnej osoby,
16. Danych szczególnie chronione - wyliczone są w art. 27 ust. 1 ustawy. Są to ***informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, religijnych, filozoficznych, wyznaniu, przynależności do partii lub związku, stanie zdrowia, kodzie genetycznym, nałogach, postępowaniu przed sadem lub urzędem***. Na administratorów tych danych ustawa nakłada bardziej rygorystyczne obowiązki, niż na administratorów danych „zwykłych”,
17. Danych **„zwykłych”-** nie jest to pojecie zdefiniowane w ustawie o ochronie danych osobowych. Pojęcie to obejmuje dane osobowe, których nie zalicza się do danych wrażliwych. Są to więc wszystkie dane osobowe poza wymienionymi w art. 27 ust. 1 ustawy. Zalicza się do nich np. ***imię, nazwisko, adres zamieszkania, datę urodzenia, nr PESEL, adres email,***
18. Zgodzie na przetwarzanie danych osobowych- należy przez to rozumieć zgodę osoby, której dane dotyczą – rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Wyrażenie zgody na przetwarzanie danych osobowych jest zbędne, gdy przetwarzanie danych jest dopuszczalne na podstawie: odrębnych przepisów lub innych przesłanek (np. w celu realizacji umowy),
19. Usuwaniu danych osobowych - należy przez to rozumieć zniszczenie danych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Usuwanie danych oznacza więc takie procedury, których zastosowanie pozbawi administratora danych możliwości jakiegokolwiek dalszego przetwarzania danych osobowych.

§ 3. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym odpowiadają w Urzędzie Gminy Wydminy:

1) Administrator Danych Osobowych,
2) Administrator Bezpieczeństwa Informacji,
3) Administrator Systemów Informatycznych,
4) Każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz Administratora Danych Osobowych, która uzyskała upoważnienie do przetwarzania danych osobowych.

II - Zasady przetwarzania i ochrony danych osobowych

§ 4. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Urzędzie jest zobowiązana do zapoznania się z niniejszym dokumentem.

§ 5. Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Urząd, przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi,

świadomymi lub nieświadomymi.

§ 6. Polityką bezpieczeństwa objęte są dane osobowe, którymi są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

§ 7. Reguły i zasady do przetwarzania danych osobowych prowadzonych zarówno w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jaki w systemach informatycznych obowiązują także w przypadku przetwarzania danych poza zbiorem danych.

§ 8. Integralną częścią polityki bezpieczeństwa są niniejsze dokumenty:

1) Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe i dane wrażliwe ***(Załącznik nr 1),***
2) Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych ***(Załącznik nr 2,.***
3) Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi ***(Załącznik nr 3,.***
4) Sposób przepływu danych pomiędzy poszczególnymi systemami ***(Załącznik nr 4),***
5) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczania przetwarzanych danych ***(Załącznik nr 5,.***
6) Obowiązki pracownicze osób zatrudnionych przy przetwarzaniu danych osobowych i danych wrażliwych wynikające z potrzeby zapewnienia ochrony danych osobowych ***(Załącznik nr 6).***

§ 9. Osoby, które przetwarzają w Urzędzie dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych osobowych nadane przez ADO ***(załącznik nr 7)*** zawierające oświadczenie o zachowaniu poufności tych danych. Osoby upoważnione do przetwarzania danych mają obowiązek:

1) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem,
2) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym,
3) zabezpieczać je przed zniszczeniem.

§ 10. W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w § 3, które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności ***(Załącznik nr 8).***

§ 11. Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych zgodnie z art. 31 ustawy. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 12. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego. Dane osobowe mogą być udostępniane osobom i podmiotom, zgodnie z przepisami prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 13. Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

1) adresat wniosku (administrator danych),
2) wnioskodawca,
3) podstawa prawna (wskazanie potrzeby),

4) wskazanie przeznaczenia,
5) zakres informacji.

§ 14. Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 15. Każda osoba fizyczna, której dane są przetwarzane w Urzędzie, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 16. W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, wyznaczona przez Administratora Danych Osobowych osoba przygotowuje odpowiedź w ciągu 30 dni.

§ 17. W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator Danych Osobowych (lub osoba przez niego wyznaczona) jest obowiązana poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy Administratorem Danych Osobowych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

§ 18. Nadzór nad przetwarzaniem danych osobowych w Urzędzie sprawuje ABI wyznaczony przez ADO. ADO jest zobowiązany zgłosić do rejestracji GIODO powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od jego powołania lub odwołania. W przypadku niewyznaczenia ABI, funkcje mu przypisane pełni ADO osobiście. Upoważnienie wyznaczające ABI stanowi ***załącznik nr 9*** do niniejszego dokumentu. ABI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik do niniejszego dokumentu.

§ 19. Do zadań ABI należy w szczególności:

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania, które za pośrednictwem administratora danych zostaje przekazane GIODO,
2) nadzorowanie opracowania i aktualizowanie dokumentacji opisującej sposób przetwarzania danych osobowych oraz przestrzeganie zasad w niej określonych,
3) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
4) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych oraz, kiedy jest to wymagane przez przepisy, zgłaszanie zbiorów do rejestracji do GIODO,
5) wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

§ 20. ABI prowadzi również następujące wykazy:

1) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych,
2) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania ***(załącznik nr 1),***

3) wykaz zbioru danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych ***(załącznik nr 2,)***
4) wykaz podmiotów i osób, którym udostępniono dane,
5) wykaz podmiotów, którym powierzono dane osobowe do przetwarzania.

§ 21. Nadzór nad przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym sprawuje ASI.

§ 22. Funkcję ASI pełni osoba wyznaczona przez ADO. ADO może każdorazowo odwołać ASI. W przypadku niewyznaczenia osoby na stanowisko ASI obowiązki dla niego przewidziane wykonuje ABI.

§ 23. Do zadań ASI należy w szczególności:

1) nadzór nad właściwym zabezpieczeniem sprzętu, w których przetwarzane są dane osobowe,
2) nadzór nad wykorzystywaniem w Urzędzie oprogramowania i jego legalnością,
3) przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przechowywane są dane osobowe,
4) podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych,
5) badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
6) podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych,
7) nadzór nad wykorzystywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem przydatności,
8) wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

III Tryb i sposób sprawdzania zgodności przetwarzania danych osobowych z obowiązującymi przepisami

§ 24. Sprawdzanie o którym mowa w § 19 pkt. 1 przeprowadzane jest w trybie

1) sprawdzenia planowanego - według planu sprawdzeń,
2) sprawdzenia doraźnego, w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez administratora bezpieczeństwa informacji wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takich naruszeń,
3) art. 19 b ust. 1 ustawy- w przypadku zwrócenia się o dokonanie sprawdzenia przez GIODO.

§ 25. Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.

§ 26. ABI w planie sprawdzeń uwzględnia w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:

1) z zasadami przetwarzania danych osobowych, o których mowa u stawie,
2) z zasadami dotyczącymi zabezpieczania danych osobowych, o których mowa w ustawie,
3) z zasadami przekazywania danych osobowych, o których mowa w ustawie, z obowiązkiem zgłaszania zbioru danych osobowych do rejestracji i jego aktualizacji, o których mowa w ustawie,

§ 27. Plan sprawozdań jest przygotowany przez ABI na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

§ 28. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczenia danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat.

§ 29. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez ABI o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

§ 30. ABI zawiadamia ADO o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia w trybie, o którym mowa w art. 19b ust. 1 ustawy, przed podjęciem pierwszej czynności w toku sprawdzania.

§ 31. ABI dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

§ 32. Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:

1) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych,
2) odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem,
3) sporządzeniu kopii otrzymanego dokumentu,
4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych,
5) sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

§ 33. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności ABI mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, w szczególności osoby zarządzającej tym systemem.

§ 34. Materiały sporządzane w postaci papierowej lub w postaci elektronicznej.

§ 35. Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia ABI przeprowadzenie czynności w toku sprawdzenia.

§ 36. ABI zawiadamia ADO o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

§ 37. Zawiadomienia nie przekazuje się w przypadku:

1) sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce,
2) sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor, jeżeli na zawiadomienie

nie pozwala wyznaczony przez niego termin.

§ 38. Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie.

§ 39. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.

§ 40. ABI przekazuje ADO sprawozdanie:
1) ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia,
2) ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia,
3) ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor – zachowując termin wskazany przez Generalnego Inspektora zgodnie z art. 19b ust. 1 ustawy.

§ 41. Nie rzadziej niż raz na rok bezpieczeństwo informacji danych osobowych w Urzędzie poddawane jest okresowemu audytowi wewnętrznemu zgodnie z obowiązującymi przepisami.

IV -Tryb i sposób nadzoru nad dokumentacją przetwarzania danych

§ 42. Sprawując nadzór, administrator bezpieczeństwa informacji dokonuje weryfikacji:
1) opracowania i kompletności dokumentacji przetwarzania danych,
2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa,
3) stanu faktycznego w zakresie przetwarzania danych osobowych,
4) zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych,
5) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

§ 43. ABI przeprowadza weryfikację:

1) w sprawdzeniach,
2) poza sprawdzeniami, na podstawie zgłoszenia osoby wykonującej obowiązki określone w dokumentacji przetwarzania danych oraz własnego udziału administratora bezpieczeństwa informacji w procedurach w niej określonych.

§ 44. ABI może przeprowadzić weryfikację poza sprawdzeniami, na podstawie zgłoszenia osoby trzeciej.

V - Instrukcja alarmowa (postępowanie w przypadku naruszenia ochrony danych osobowych)

§ 45. Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:
1) próby naruszenia ochrony danych osobowych:
    a) − z zewnątrz - włamania do systemu, podsłuch, kradzież danych,
    b) − z wewnątrz- nieumyślna lub celowa modyfikacja danych, kradzież danych.
2) programy destrukcyjne:
    a) − wirusy,
    b) − konie trojańskie,
    c) − makra,
    d) − bomby logiczne
3) awarie sprzętu lub oprogramowania,
4) zabór sprzętu lub uszkodzenie oprogramowania,
5) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,

6) usiłowanie zakłócenia działania systemu informatycznego.

§ 46. W przypadku stwierdzenia faktu nieprawidłowego przetwarzania, ujawnienia lub nienależytego zabezpieczenia przed osobami nieupoważnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych, każdy pracownik Ośrodka, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa jest zobowiązany fakt ten niezwłocznie zgłosić ABI. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji należy powiadomić osobę przez niego upoważnioną.

§ 47. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych lub danych wrażliwych ABI lub upoważnionej przez niego osoby, należy:
1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyny lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać- o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby upoważnionej.

§ 48. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych i danych wrażliwych, ABI lub osoba go zastępująca:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Ośrodka,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) rozważa celowości potrzebę powiadomienia o zaistniałym naruszeniu ADO,
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami z jednostki nadrzędnej (Urząd Gminy) lub pracownikami z firm specjalistycznych.

§ 49. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 10, który powinien zawierać w szczególności:
1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu i miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania, wstępna ocenę przyczyn wystąpienia naruszenia,
5) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

§ 50. Raport, o którym mowa w § 5, ABI niezwłocznie przekazuje ADO, a w przypadku jego nieobecności osobie uprawnionej.

VI - Szkolenie użytkowników

§ 51. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

§ 52. Za przeprowadzenie szkolenia oraz jego zorganizowanie odpowiada ABI.

§ 53. Przeszkolenie odbywa się poprzez zapoznanie użytkowników z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym.

VII - Postanowienia końcowe

§ 54. Użytkownicy są obowiązani zapoznać się z treścią polityki oraz do jej stosowania przy przetwarzaniu danych osobowych.

§ 55. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

§ 56. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

§ 57. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 58. W sprawach nieuregulowanych w niniejszej polityce mają zastosowanie przepisy ustawy oraz wydanej na jej podstawie akty wykonawcze.

Załącznik Nr 1
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

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

Pokój nr 2
- Urząd Stanu Cywilnego
- Ewidencja ludności
- Rejestr wyborców

Pokój nr 3
- Dowody osobiste

Pokój nr 4
- Kadry

Pokój nr 8
- Działalność gospodarcza
- Zagospodarowanie przestrzenne
- Gospodarka mieniem gminy
- Ochrona środowiska

Pokój nr 21
- Podatki i windykacja podatkowa

Pokój nr 23 (sekretariat)
- Rejestr korespondencji

Załącznik Nr 2
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

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

1. Politykę Bezpieczeństwa stosuje się do:

A. danych osobowych przetwarzanych w systemie PUMA
   - Ewidencja ludności
   - Rejestr wyborców
   - Kadry
   - Płace
   - Kontrahent (Podatki od osób fizycznych, Windykacja podatkowa, Najemcy i dzierżawcy mienia komunalnego)

B. danych osobowych przetwarzanych w systemie Płatnik,

C. danych osobowych przetwarzanych w formie dokumentów Excel (rejestr decyzji o ustaleniu warunków zabudowy, dziennik korespondencji i listy adresowe w korespondencji seryjnej)

D. wszystkich informacji dotyczących danych pracowników Urzędu Gminy Wydminy, w tym danych osobowych i treści zawieranych umów o pracę,

E. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,

F. rejestru osób dopuszczonych do przetwarzania danych osobowych,

G. innych dokumentów zawierających dane osobowe.

Załącznik Nr 3
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

I. PUMA – system informatyczny oparty o wspólną bazę danych zawierającą informacje dotyczące:

1. **Ewidencja ludności**

nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, seria i numer dowodu osobistego, stan cywilny, obywatelstwo,

2. **Rejestr wyborców**

nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL,

3. **Kadry**

nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, stan cywilny, obywatelstwo, nr rachunku bankowego, stan rodzinny, stan zdrowia, karalność, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym.

4. **Kontrahent**

nazwiska i imiona, numer ewidencyjny PESEL, NIP, numer telefonu, stan cywilny, powierzchnia prowadzonego gospodarstwa rolnego, nr rachunku bankowego, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym.

5. **Podatki od osób fizycznych**

nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, powierzchnia prowadzonego gospodarstwa rolnego, nr rachunku bankowego.

6. **Windykacja podatkowa**

nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, powierzchnia prowadzonego gospodarstwa rolnego, nr rachunku bankowego.

II. **Najemcy i dzierżawcy mienia komunalnego**

nazwiska i imiona, adres zamieszkania lub pobytu właścicieli, współwłaścicieli, najemców i dzierżawców – listy i arkusze kalkulacyjne (xls),

III. **Dziennik korespondencyjny i listy adresowe**

nazwiska i imiona, adres zamieszkania – listy i arkusze kalkulacyjne (xls).

IV. **Rejestr decyzji o ustaleniu warunków zabudowy, lokalizacji inwestycji celu publicznego i podziałów nieruchomości**

Obręb geodezyjny, numer nieruchomości, imię i nazwisko wnioskodawcy – listy i arkusze kalkulacyjne (xls).

Załącznik Nr 4
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

Przepływ danych pomiędzy systemami

Systemy, w których przetwarzane są dane osobowe są niezależne i posiadają samodzielne bazy danych. Istnieją możliwości generowania z systemu **PUMA** plików XML do zaimportowania przez system **Besti@, Płatnik oraz system bankowy.**

Załącznik Nr 5
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

§ 1

Dane osobowe z użyciem systemu informatycznego i w formie papierowej są przetwarzane w godzinach pracy Urzędu Gminy Wydminy. Poza tymi godzinami wyłącznie w uzasadnionych przypadkach, po uzyskaniu zgody administratora danych i powiadomieniu administratora bezpieczeństwa informacji.

§ 2

W obszarze przetwarzania danych osobowych mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych, osoby zainteresowane przetwarzanymi danymi, Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego oraz inne osoby indywidualnie upoważnione do tego przez Administratora Danych Osobowych. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania tych danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.

§ 3

Okna pomieszczeń znajdujących się w budynku posiadają zabezpieczenia w postaci klamek wewnętrznych.

§ 4

Pomieszczenia w obszarze przetwarzania danych osobowych są zamykane na zamek w czasie nieobecności pracowników. Klucze są przechowywane w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione do przetwarzania danych osobowych.

§ 5

Dokumenty papierowe przechowywane są w szafach zamykanych na klucz. Przechowywane są zgodnie z Instrukcją kancelaryjną. Klucze do szaf z dokumentami przechowują osoby upoważnione do przetwarzania danych osobowych

§ 6

Monitory komputerów, na których odbywa się przetwarzanie danych osobowych w sposób informatyczny są zlokalizowane w sposób uniemożliwiający osobom trzecim podgląd wyświetlanych danych. Konfiguracja wyświetlania obrazu na monitorach komputerów musi zawierać włączenie wygaszacza ekranu po zadanym czasie (5 minut) lub w przypadku braku wygaszacza ekranu wyłączenie monitora w przypadku braku aktywności użytkownika (5 minut). Zaleca się, aby powrót do pracy po okresie bezczynności wymagał podania hasła dostępu (np. hasło wygaszacza ekranu).

§ 7

Dyski HDD i inne nośniki elektroniczne zawierające dane osobowe przeznaczone do likwidacji, naprawy są przed opuszczeniem Urzędu Gminy Wydminy pozbawiane zapisu lub niszczone fizycznie (jeżeli nie ma innej metody zlikwidowania zapisu).

§ 8

Sieć komputerowa Urzędu Gminy Wydminy podłączona jest do sieci Internet. Dostęp do zasobów sieci Internet posiadają tylko osoby, którym jest to konieczne do wykonywania obowiązków służbowych.

§ 9

Wydruki komputerowe zawierające dane osobowe, a przeznaczone do likwidacji są niszczone w sposób bezpowrotny tak, aby nie było możliwości odczytania zamieszczonych na nich informacji poprzez spalenie.

§ 10

W celu ochrony antywirusowej stosuje się oprogramowanie antywirusowe z codzienną aktualizacją baz wirusów.

Załącznik Nr 6
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

Obowiązki pracownicze osób zatrudnionych przy przetwarzaniu danych osobowych wynikające z przyczyn zapewnienia ochrony danych osobowych

§ 1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do zbiorów danych osobowych.

§ 2. Naruszenie zasad ochrony danych osobowych, w szczególności umyślne lub nieumyślne udostępnianie danych osobowych osobie nieupoważnionej, jest naruszeniem obowiązków pracowniczych. W tym przypadku zastosowanie mają przepisy z art. 51, 52 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922).

§ 3. Kierownik referatu właściwego obowiązany jest do:

1) Kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników,
2) Zapewnienia, że przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych Osobowych bądź Administratora Bezpieczeństwa Informacji w zakresie indywidualnych obowiązków pracowniczych.

§ 4. Osoba upoważniona przez Administratora Danych Osobowych bądź Administratora Bezpieczeństwa Informacji jest zobowiązana do:

1) Zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
2) Stosowania określonych przez administratora danych procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
3) Zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych,
4) Przestrzegania ustalonych zasad i procedur w zakresie ochrony danych osobowych.

Załącznik Nr 7
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1.Upoważniam Pani/Pana .....

o numerze PESEL .....

zatrudnioną/-ego na stanowisku .....

w Urzędzie Gminy Wydminy

do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:

(należy określić zbiory zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa)

–.....

–.....

2.Identyfikator/Login: .....

3.Okres trwania upoważnienia: .....

Wystawił.....

4.Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

….....
(Data i podpis osoby upoważnione)j

……
(podpis Administratora Danych Osobowych lub ABI
zgodnie z Polityką Bezpieczeństwa)

Załącznik Nr 8
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Urzędu Gminy Wydmin. Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

…….....
(Data i podpis osoby składającej oświadczenie)

Załącznik Nr 9
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

UPOWAŻNIENIE DLA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI (ABI)

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016r. poz. 922), z dniem..... wyznaczam Administratora Bezpieczeństwa Informacji i powierzam tę funkcję Panu/Pani.....posługującemu/-ej się numerem PESEL:.....

Do obowiązków Administratora Bezpieczeństwa Informacji będzie należało wdrożenie i nadzór nad prawidłową realizacją Polityki Bezpieczeństwa obowiązującej w jednostce organizacyjnej, w szczególności:

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania, które za pośrednictwem administratora danych zostaje przekazane GIODO,
2) nadzorowanie opracowania i aktualizowanie dokumentacji opisującej sposób przetwarzania danych osobowych oraz przestrzeganie zasad w niej określonych,
3) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
4) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych oraz, kiedy jest to wymagane przez przepisy, zgłaszanie zbiorów do rejestracji do GIODO,
5) wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych, n)prowadzenie ewidencji osób, którym nadano upoważnienia do przetwarzania danych osobowych ,
6) wyznaczanie Administratora Systemu Informatycznego (ASI) p)nadawanie upoważnienia do przetwarzania danych osobowych

.....
(podpis Administratora Danych Osobowych)

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Administratora Bezpieczeństwa Informacji w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ustawę o ochronie danych osobowych oraz rozporządzenie wykonawcze wydane na podstawie art. 39a do wyżej wymienionej ustawy.

….....
(podpis Administratora Bezpieczeństwa Informacji /ABI/)/

Załącznik Nr 10
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w Urzędzie Gminy Wydminy

RAPORT z naruszenia bezpieczeństwa systemu informatycznego
w Urzędzie Gminy Wydminy

1. Data: ..... Godzina: ..... *(dd.mm.rr.) (gg.mm.)*

1.Osoba powiadamiająca o zaistniałym zdarzeniu:
.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

2.Lokalizacja zdarzenia: .....
(np. nr pokoju, nazwa pomieszczenia)

3.Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
.....
.....
.....
.....

4.Przyczyna wystąpienia zdarzenia:
.....
.....
.....
.....

5.Podjęte działania:
.....
.....
.....
….....

6.Postępowanie wyjaśniające:
.....
.....
.....
.....

….....
(data, podpis Administratora Bezpieczeństwa Informacji)