Załącznik Nr 2
do Zarządzenia Nr 102/2016
Wójta Gminy Wydminy
z dnia 6 grudnia 2016r

Instrukcja zarządzania systemem informatycznym Urzędu Gminy Wydminy

I – Część ogólna

Na podstawie przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922) oraz 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 informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024).

§ 1. 1. Instrukcja zarządzania systemem informatycznym Urzędu Gminy Wydminy, zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.

2. Niniejsza instrukcja realizuje „Politykę bezpieczeństwa przetwarzania danych osobowych" obowiązującą w **Urzędzie Gminy Wydminy**.

§ 2. Ilekroć w niniejszym dokumencie jest mowa o:

1) Urzędzie- należy przez to rozumieć Urząd Gminy Wydminy,
2) ustawie- należy przez to rozumieć ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922),
3) ADO - należy przez to rozumieć Administratora Danych Osobowych w rozumieniu ustawy, Administratorem Danych jest Urząd Gminy Wydminy. W imieniu Administratora Danych obowiązki określone w Ustawie pełni Administrator Bezpieczeństwa Informacji (ABI).
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", obowiązująca 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) incydencie - należy przez to rozumieć naruszenie bezpieczeństwa informacji ze względu na poufność, dostępności integralność,
10) 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 cywilnoprawnej, osoba odbywająca staż w Urzędzie,
11) identyfikatorze użytkownika – należy przez to rozumieć ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
12) sieci lokalnej – należy przez to rozumieć połączenie komputerów pracujących w Urzędzie, w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,
13) sieci publicznej – należy przez to rozumieć sieć telekomunikacyjną, nie będąca siecią wewnętrzną, służącą do świadczenia usług telekomunikacyjnych, w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.),
14) sieci telekomunikacyjnej – należy przez top rozumieć urządzenia

telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną, w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.),

15) systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych,

16) słabości systemu - należy przez to rozumieć zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu,

17) działaniu korygującym - należy przez to rozumieć działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności/ incydentu lub innej potencjalnej sytuacji,

18) działaniu zapobiegawczym - należy przez to rozumieć działanie które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnych niezgodności/ incydentów lub innej potencjalnej sytuacji niepożądanej,

19) przetwarzaniu danych – należy przez to rozumieć jakiekolwiek operacje, wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,

20) zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

21) teletransmisji – należy przez to rozumieć przesyłanie informacji za pomocą sieci telekomunikacyjnej,

22) aplikacji – należy przez to rozumieć program komputerowy, wykonujący konkretne zadanie,

23) wysokim poziomie bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną,

24) 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,

25) tożsamości – oznacza cechy, które stanowią o tym, kim dana osoba jest, czym różni się od innych. Na tak rozumianą tożsamość składa się nie tylko to, kim się jest obecnie, ale także to kim się było, a nawet zamierzenia na przyszłość, wszystko to powoduje, że dana osoba różni się od innej

26) danych szczególnie chronionych- dane 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”.

27) 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,

28) 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 prawa (np. w celu przeprowadzenia wywiadu środowiskowego przez pracownika pomocy społecznej) lub innych przesłanek (np. w celu realizacji umowy),

29) 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,

30) korekcji - należy przez to rozumieć działanie w celu wyeliminowania wykrytej niezgodności lub incydentu,

31) kontroli (audycie) - systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań, polityk i procedur.

§ 3. ASI wyznaczany jest przez ABI lub ADO drogą pisemnego upoważnienia. W przypadku nie wyznaczenia ASI, jego funkcję pełni ABI lub osoba pełniąca funkcję ABI. Wzór upoważnienia ASI stanowi załącznik nr 1 do niniejszego dokumentu. ASI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 8 do Polityki Bezpieczeństwa.

§ 4. ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu. Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego. Obowiązkiem ASI jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

§ 5. Zgodnie z rozporządzeniem, uwzględniając fakt, że użytkowany w jednostce organizacyjnej system informatyczny służący do przetwarzania danych osobowych jest połączony z siecią Internet, wprowadza się wysoki poziom bezpieczeństwa.

II - Część szczegółowa

§ 6. 1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

1) ustawą,
2) Polityką Bezpieczeństwa,
3) niniejszym dokumentem, oraz posiadać upoważnienie do przetwarzania danych osobowych.

2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik Nr 2.

§ 7. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym określa się w sposób następujący:

1) użytkownik zamierzający przetwarzać dane osobowe, po uzyskaniu upoważnienia stanowiącego załącznik nr 7 do Polityki, oraz podpisaniu oświadczenia stanowiącego załącznik nr 8 do Polityki, składa wniosek o nadanie dostępu do systemu informatycznego stanowiącego załącznik nr 3,
2) w przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia, stanowiącego załącznik nr 7 do Polityki Bezpieczeństwa, ASI zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.
3) przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakres dostępu danych i operacji.
4) ASI zobowiązany jest niezwłocznie przydzielić użytkownikowi identyfikator i hasło. Podanie użytkownikowi hasła nie może nastąpić w sposób umożliwiający zapoznanie się z nim osobom trzecim.

§ 8. Stosuje się następujące metody oraz środki uwierzytelniania, a także procedury związane z ich zarządzaniem i użytkowaniem:

1) osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest ASI,
2) użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła, jest również zobowiązany do zmiany hasła, co każde 30 dni,
3) przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła - 8 znaków,
   b) zakazuje się stosować: haseł, które użytkownik stosował uprzednio, swojego identyfikatora w jakiejkolwiek formie, swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku (numer telefonu, numer rejestracyjny samochodu, numer PESEL, itp.),
   c) należy stosować: hasła zawierające kombinacje liter i cyfr, hasła zawierające znaki specjalne (():'@,#,& itp.) o ile system informatyczny i oprogramowanie na to pozwala,
   d) zmiany hasła nie wolno zlecać innym osobom.
4) użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich,
5) pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony,
6) pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
7) odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika referatu z podaniem daty oraz przyczyny odebrania uprawnień,
8) Kierownik referatu zobowiązany jest pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
9) identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym oraz unieważnić hasło,
10))identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może zostać przydzielany innej osobie.
11))hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie Administratora Bezpieczeństwa Informacji.
12) ASI zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym. Rejestr stanowi załącznik Nr 4.

§ 9. Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

1) rozpoczęcie pracy w systemie komputerowym wymaga zalogowania się do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu,
2) przed opuszczeniem stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i systemu operacyjnego,
3) system jest skonfigurowany w taki sposób, aby po okresie 5 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu hasła,
4) przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów, wylogować się z systemu operacyjnego i wykonać zamknięcie systemu,
5) niedopuszczalne jest włączanie komputera przed zamknięciem oprogramowania i systemu operacyjnego.

§ 10. Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1) za systematyczne przygotowanie kopii bezpieczeństwa odpowiada ASI,
2) kopie bezpieczeństwa wykonywane są codziennie,

3) kopie bezpieczeństwa wykonywane są na serwerze głównym urzędu.

§ 11. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków:

1) Elektroniczne nośniki informacji:
    a) dane osobowe w postaci elektronicznej – za wyjątkiem kopii bezpieczeństwa – zapisane na płytach CD/DVD nie mogą opuścić obszaru przetwarzania danych osobowych,
    b) elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych, w zamkniętych szafach,
    c) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a następnie uszkadza się w sposób mechaniczny,
    d) elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do dostępu do tych danych, nawet po uprzednim usunięciu danych z nośnika,
    e) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
2) Kopie zapasowe:
    a) kopie bezpieczeństwa są przechowywane na serwerze Urzędu Gminy Wydminy,
    b) dostęp do danych opisanych w punkcie 1 ma ASI oraz upoważnieni pracownicy.
3) Wydruki:
    a) w przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym,
    b) pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy,
    c) wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 12. System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania, o jakim mowa w pkt. 1 niniejszego paragrafu:

1) oprogramowaniem antywirusowym stosowanym w Urzędzie jest G-Data Internet Security,
2) użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła bez zgody ASI,
3) za wdrożenie i korzystanie z oprogramowania antywirusowego, określonego w **pkt 1** oraz oprogramowania firewall, odpowiada ASI

§ 13. Stosuje się następujące procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1) ASI w terminach określonych przez producenta sprzętu wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z niniejszej Instrukcji
2) w przypadku stwierdzenia przez ASI nieprawidłowości w działaniu elementów systemu opisanych w lit. a niniejszego paragrafu podejmuje on niezwłocznie czynności służące do przywrócenia ich prawidłowego działania
3) jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI lub w sytuacji

wyjątkowej – osoby przez niego wyznaczonej
4) o fakcie ujawnienia nieprawidłowości należy zawiadomić ASI,
5) konserwacja baz danych osobowych przeprowadzona jest zgodnie z zaleceniami twórców poszczególnych programów,
6) ASI zobowiązany jest uaktywnić mechanizm zaliczania nieudanych prób dostępu do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.

§ 14. System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie:
1) urządzeń UPS,
2) listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami.

§ 15. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
2) przekazanie podmiotowi nieuprawnionemu do przetwarzania danych- pozbawia się wcześniej zapisu tych danych,
3) naprawy- pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.

§ 16. W przypadku jakichkolwiek nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia o uszkodzenie sprzętu, oprogramowania lub danych należy bezzwłocznie
powiadomić bezpośredniego przełożonego, który zawiadamia ABI w celu:
1) w przypadku włamania lub podejrzenia włamania do systemu administrator danego systemu podejmuje działania w celu zabezpieczenia systemu i danych:
   a) zmienia hasło administracyjne,
   b) określa rodzaj i sposób włamania,
   c) podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu, szacuje straty w systemie,
   d) przywraca stan systemu przed włamaniem.
2) w przypadku uszkodzenia sprzętu lub programów z danymi administrator danego systemu podejmuje działania w celu:
   a) określenie przyczyn uszkodzenia,
   b) oszacowanie strat wynikłych z w/w uszkodzenia,
   c) naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego zainstalowania danego programu, odtworzenie jego pełnej konfiguracji oraz wczytanie danych z ostatniej kopii zapasowej,
3) w przypadku uszkodzenia danych administrator systemu podejmuje następujące działania:
   a) ustala przyczynę uszkodzenia danych,
   b) określa wielkość i jakość uszkodzonych danych,
   c) podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej

§ 17 W przypadku stwierdzenia nieprawidłowości w funkcjonowaniu sieci telekomunikacyjnej każdy użytkownik zobowiązany jest niezwłocznie powiadomić administratora sieci, który podejmuje działania w celu ustalenia przyczyn zaistniałej sytuacji oraz wyeliminowania nieprawidłowości.

§ 18 Wszystkie działania konserwacyjne, awarie oraz napraw powinny być rejestrowane w prowadzonym „Dzienniku systemu informatycznego Urzędu Gminy Wydminy". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku Nr 5. Wpisów do dziennika może dokonywać Administrator Danych Osobowych, Administrator Bezpieczeństwa Informacji lub osoby przez nich wyznaczone.

III -Postanowienia końcowe

§ 19 W sprawach nieuregulowanych niniejszą Instrukcją znajdują zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922) Rozporządzenie 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 informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024 z późn. zm.).

Załącznik Nr 1
do Instrukcji Zarządzania Systemem Informatycznym
w Urzędzie Gminy Wydminy

.....
miejscowość, data

UPOWAŻNIENIE DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO(ASI)

Na podstawie części I §3 Instrukcji Zarządzania Systemem Informatycznym, z dniem.....wyznaczam Administratora Systemu Informatycznego **(ASI),** powierzając tę funkcję Panu/Pani..... posługującemu/-ej się numerem PESEL: .....

.....
podpis Administratora Bezpieczeństwa Informacji
lub Administratora Danych Osobowych

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Administratora Systemu Informatycznego w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ze szczególnym uwzględnieniem obowiązków przewidzianych w części I §4 Instrukcji Zarządzania Systemem Informatycznym.

.....
podpis Administratora Systemu Informatycznego (ASI)

Załącznik Nr 2
do Instrukcji zarządzania systemem informatycznym
w Urzędzie Gminy Wydminy

Oświadczenie

Oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016r. poz. 922 ze zm.),

2. 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 informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100 poz. 1024),

3. Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Wydminy,

4. Instrukcji zarządzania systemem informatycznym Urzędu Gminy Wydminy. Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:

- Zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Urzędu Gminy Wydminy, zabezpieczenia przed udostępnieniem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.

- Zachowaniem w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych oraz haseł dostępu do tych zbiorów.

Wydminy, dn. ..... **.....**
(podpis pracownika)

Załącznik Nr 3
do Instrukcji zarządzania systemem informatycznym
w Urzędzie Gminy Wydminy

Wniosek o nadanie uprawnień w systemie informatycznym

Rodzaj zmiany w systemie informatycznym:

….....Nowy użytkownik ….....Modyfikacja uprawnień ….....Odebranie uprawnień

Imię i nazwisko użytkownika ….....

Opis zakresu uprawnień użytkownika w systemie informatycznym:

….....
.....
.....
.....
.....

Data wystawienia: .....

Podpis użytkownika:.....

…… ……

(podpis Kierownika) (Akceptacja ABI)

Załącznik Nr 4
do Instrukcji zarządzania systemem informatycznym
w Urzędzie Gminy Wydminy

Ewidencja osób upoważnionych do pracy w systemie informatycznym oraz upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko i imię (Identyfikator)	System/aplikacja zbiór danych osobowych	Data nadania upoważnienia	Data ustania upoważnienia

Załącznik Nr 5
do Instrukcji zarządzania systemem informatycznym
w Urzędzie Gminy Wydminy

Dziennik systemu informatycznego Urzędu Gminy w Wydminach

Dziennik zawiera opis wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:
w przypadku awarii – opis awarii, przyczynę awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
w przypadku konserwacji systemu – opis podjętych działań, wnioski.

Lp.	Data i godzina zdarzenie	Opis zdarzenia	Podjęte działania	Podpis
1				
2				
3				
4				
5				
6				
7				
8				