Zarządzenie Nr 89/2015
Wójta Gminy Piekoszów
z dnia 10 sierpnia 2015r.

w sprawie powołania oraz powierzenia obowiązków i odpowiedzialności Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Piekoszowie

Na podstawie art. 33 ust. 1, 3 i 5 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2013r. poz. 594 ze zm.) art.36a, art.37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U z 2014r. poz.1182 ze zm.) oraz § 6 ust.6 i § 13 ust.1 pkt 12 Regulaminu Organizacyjnego Urzędu Gminy w Piekoszowie nadanego zarządzeniem Nr 25/2013 Wójta Gminy Piekoszów z dnia 26.04.2013r. ze zmianami, a także §1 pkt 1 załącznika Nr 1 do w/w Regulaminu Organizacyjnego Urzędu Gminy **zarządza się, co następuje:**

§1.1. Powołuje się Pana Marcina Podlasińskiego zatrudnionego na stanowisku informatyka w Referacie Organizacyjnym i Spraw Obywatelskich na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy w Piekoszowie.

2. Zakres obowiązków i odpowiedzialności Administratora Bezpieczeństwa Informacji stanowi załącznik do zarządzenia.

§2. Upoważnia się Pana Marcina Podlasińskiego do przetwarzania danych osobowych zgromadzonych w Urzędzie Gminy w Piekoszowie.

§3. Poza obowiązkami i odpowiedzialnością, o których mowa w § 1 powierza się Panu Marcinowi Podlasińskiemu obowiązki i odpowiedzialność w zakresie:

1) terminowego i rzetelnego sporządzania sprawozdań o zgodności przetwarzanych danych osobowych z przepisami ustawy, obejmujących dane zawarte w art.36c ustawy,
2) kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
3) prowadzenia ewidencji osób upoważnionych do przetwarzania danych zawierającą:
   a) imię i nazwisko osoby upoważnionej;
   b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
   c) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
4) zgłaszania zbiorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a ustawy,
5) prawidłowego stosowania przepisów rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015r. poz.745)

§4. W zakresie obowiązków i realizacji zadań związanych z ochroną danych osobowych Administrator Bezpieczeństwa Informacji podlega bezpośrednio Wójtowi Gminy Piekoszów.

§5. Zarządzenie wchodzi w życie z dniem podpisania.

Po zapoznaniu się z treścią niniejszego Zarządzenia potwierdzam, że przyjmuję zakres obowiązków i odpowiedzialności w nim określony:

13.08.2015 Marcin Podlasiński
(imię i nazwisko, data i podpis pracownika)

Otrzymują:
1) adresat ; 2) a/a osobowe; 3) Ref. ORG x2 (rejestr i zbiór)

SEKRETARZ GMINY
mgr Grażyna Tatar

Załącznik
do zarządzenia Nr 89/2015
Wójta Gminy Piekoszów
z dnia 10 sierpnia 2015r.

Zakres obowiązków i odpowiedzialności
Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Piekoszowie

§1. Zapewnienie przestrzegania w Urzędzie Gminy w Piekoszowie przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych, w szczególności poprzez:

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora danych,
2) opracowywanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzeganie zasad w niej określonych,
3) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

§2. Opracowywanie i aktualizowanie dokumentacji opisującej sposób przetwarzania danych oraz zapewnienie środków technicznych i organizacyjnych gwarantujących ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, oraz przestrzeganie zasad w niej określonych, w tym Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§3. Prowadzenie nadzoru nad fizycznym zabezpieczeniem pomieszczeń, w których są przetwarzane dane osobowe oraz nad kontrolą przebywających w nich osób poprzez przygotowywanie i wydawanie imiennych identyfikatorów oraz nadawanie uprawnień do pobierania kluczy w systemie elektronicznym wraz z prowadzenie odpowiedniej ewidencji.

§4. Nadzorowanie zapewnienia awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.

§5. Nadzorowanie zabezpieczenia komputerów przenośnych hasłami dostępu przed nieuprawnionym uruchomieniem oraz przed udostepnieniem osobom nieupoważnionym do przetwarzania danych osobowych.

§6. Prowadzenie ewidencji eksploatowanych komputerów przenośnych.

§7. Prowadzenie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.

§8. Prowadzenie ewidencji dysków twardych.

§9. Zarządzanie hasłami użytkowników i nadzorowanie przestrzegania procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które są zawarte w Polityce Bezpieczeństwa Informacji.

§10. Prowadzenie ewidencji nadawanych i odbieranych uprawnień do przetwarzania danych osobowych.

§11. Nadawanie w imieniu Administratora danych upoważnień do przetwarzania danych osobowych.

§12. Prowadzenie ewidencji nadanych upoważnień do przetwarzania danych osobowych.

§13. Systematyczne sprawdzanie systemów informatycznych pod kątem obecności wirusów komputerowych, oraz aktualizowanie systemów antywirusowych i ich konfiguracji.

§14. Nadzorowanie sporządzania kopii awaryjnych oraz ich okresowe sprawdzanie pod kątem dalszej ich przydatności do odtwarzania danych w przypadku awarii systemu.

§15. Nadzorowanie systemów komunikacji elektronicznej w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji.

§16. Nadzorowanie obiegu, przechowywania oraz brakowania dokumentów zawierających dane osobowe.

§17. Nadzorowanie funkcjonowania mechanizmów uwierzytelniania użytkowników w systemach informatycznych przetwarzających dane osobowe oraz kontrolowanie dostępu do danych osobowych. Nadzorowanie to obejmuje:

1) ustalenie identyfikatorów użytkowników i ich haseł, w tym prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych,
2) czuwanie, aby hasła użytkowników były zmieniane co najmniej raz na miesiąc (analiza codziennych raportów z systemów informatycznych),
3) czuwanie, aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i hasła,
4) czuwanie, aby hasła użytkowników trzymane były w tajemnicy, również po terminie ich przydatności,
5) czuwanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zostały natychmiast wyrejestrowane, a ich hasła unieważnione.

§18. Nadzorowanie odpowiedniego ustawienia ekranów monitorów komputerowych.

§19. Udzielanie instruktażu i prowadzenie szkoleń ze wszystkimi osobami nowozatrudnionymi w Urzędzie.

§20. Przyjmowanie od osób nowozatrudnionych oświadczeń o zachowaniu danych w tajemnicy i o zapoznaniu się z obowiązującymi w Urzędzie przepisami dotyczącymi ochrony danych osobowych i bezpieczeństwa teleinformatycznego. Obowiązek ten dotyczy również osób odbywających w Urzędzie praktykę, staż itp.

§21. Prowadzenie szkoleń dla pracowników Urzędu z zakresu ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego, w szczególności po zmianie przepisów dotyczących ochrony danych osobowych.

§22. Prowadzenie korespondencji z Biurem Głównego Inspektora Ochrony Danych Osobowych w sprawach wynikających z realizacji zadań dotyczących ochrony danych osobowych.

§23. Rejestracja w GIODO zbiorów danych osobowych i ich zmian na podstawie pisemnych informacji Kierowników merytorycznych komórek organizacyjnych Urzędu w terminach wynikających z ustawy.

§24. Współpraca z merytorycznymi komórkami organizacyjnymi Urzędu przy złożonych wnioskach o udostępnienie danych osobowych.

§25. Nadzorowanie umów na udostępnianie lub powierzanie przetwarzania danych osobowych osobom lub podmiotom zewnętrznym w zakresie stosowania zapisów bezpieczeństwa przetwarzania i ochrony danych osobowych.

§26. Udzielanie wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie prowadzonych kontroli w celu dostosowania ochrony danych osobowych do stanu zgodnego z przepisami prawa.

§27. Podejmowanie działań zabezpieczających stan sytemu informatycznego w przypadku otrzymania informacji o naruszeniu jego zabezpieczeń lub informacji o zmianach w sposobie działania programu lub urządzenia wskazujących na naruszenie bezpieczeństwa danych.

§28. W przypadku wystąpienia naruszenia bezpieczeństwa danych prowadzenie analizy okoliczności i przyczyn, które do tego doprowadziły, a także przygotowywanie i przedstawianie Administratorowi danych propozycji wprowadzenia odpowiednich zmian do Polityki Bezpieczeństwa Informacji, mających na celu wyeliminowanie lub ograniczenie wystąpienia podobnych sytuacji w przyszłości.

§29. Prowadzenie audytów i kontroli w komórkach merytorycznych Urzędu oraz w miarę potrzeb w jednostkach organizacyjnych Gminy Piekoszów oraz prowadzenie sprawdzeń zaleconych przez GIODO.

§30. Po dokonaniu sprawdzeń, o których mowa w § 29 przygotowywanie i przedstawianie za pośrednictwem Administratora danych stosownych sprawozdań Generalnemu Inspektorowi Ochrony Danych Osobowych.

§31. Administrator Bezpieczeństwa Informacji przy wykonywaniu sowich zadań i obowiązków stosuje obowiązujące w tym zakresie przepisy prawne, a w szczególności:

1) ustawę z dnia 8 marca 1990r. o samorządzie gminnym,
2) ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych,
3) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji
4) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji,
5) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych,
6) 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,
7) Statut Gminy Piekoszów,
8) Regulamin Organizacyjny Urzędu Gminy w Piekoszowie,
9) Regulamin Pracy Urzędu Gminy w Piekoszowie.

§32. Pisma w sprawach dotyczących działania Administratora Bezpieczeństwa Informacji podpisuje ABI za wyjątkiem pism zastrzeżonych do podpisu innym osobom w Regulaminie Organizacyjnym Urzędu Gminy w Piekoszowie.

§33. Administrator Bezpieczeństwa Informacji wykonując swe obowiązki ma prawo żądać:

1) złożenia pisemnych lub ustnych wyjaśnień przez pracowników Urzędu lub jednostek organizacyjnych Gminy Piekoszów, w zakresie niezbędnym do ustalenia stanu faktycznego,
2) okazania dokumentów i wszelkich danych mających bezpośredni związek z ustaleniem stanu faktycznego lub problematyki kontroli prawidłowości wykonywania zadań przez pracowników Urzędu lub jednostek organizacyjnych Gminy Piekoszów,
3) udostępnienia do kontroli urządzeń, nośników, systemów informatycznych służących do przetwarzania danych od pracowników Urzędu lub jednostek organizacyjnych Gminy Piekoszów.

SEKRETARZ GMINY
mgr Grażyna Tatar