ZARZĄDZENIE Nr 26/2015
Wójta Gminy Grudusk
z dnia 17 czerwca 2015 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Gminy Grudusk.

Na podstawie art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r. poz. 594 ze zm.), art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 ze zm.), zarządzam co następuje:

§ 1

1. Wyznaczam Panią Monikę Klein na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy Grudusk.
2. Zakres działania ABI stanowi załącznik Nr 1 do niniejszego zarządzenia.

§ 2

1. Wyznaczam Pana Mariusza Krawczyka na Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Grudusk.
2. Zakres działania ASI stanowi załącznik Nr 2 do niniejszego zarządzenia .

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Jacek Oględzki

RADCA PRAWNY
Bożenna Michel-Paluszuska
WR-C-524

Załącznik Nr 1
do Zarządzenia Nr 26/2015
Wójta Gminy Grudusk
z dnia 17 czerwca 2015 r.

Zakres działania Administratora Bezpieczeństwa Informacji (ABI)

Do zadań Administratora Bezpieczeństwa Informacji należy:

1. Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2. Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
3. Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób.
4. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych.
5. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisywane są dane osobowe.
6. Nadzór nad zarządzaniem hasłami użytkowników i przestrzeganiem procedur określających częstotliwość ich zmiany.
7. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych.
8. Nadzór nad wykonywaniem kopii awaryjnych.
9. Nadzór nad systemem komunikacji w sieci komputerowej.
10. Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
11. Kontrola nad danymi osobowymi wprowadzonymi do zbiorów (przez kogo zostały wprowadzone, komu są przekazywane).
12. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń.
13. Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe.
14. Nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych.
15. Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji uprawniony jest do:

a) wydawania poleceń wszystkim pracownikom Urzędu Gminy Grudusk w zakresie związanym ze wdrożeniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.

b) rozstrzygania sporów dotyczących stosowania i interpretacji wymagań zawartych w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz wydawania wiążących decyzji w tym zakresie.

c) dostępu do wszystkich dokumentów występujących w Urzędzie Gminy Grudusk, których treść może być istotna z punktu widzenia funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji.

Załącznik Nr 2
do Zarządzenia Nr 26/2015
Wójta Gminy Grudusk
z dnia 17 czerwca 2015 r.

Zakres działania Administratora Systemów Informatycznych w Urzędzie Gminy Grudusk.

Do zadań Administratora Systemów Informatycznych należy:

1. Nadawanie identyfikatorów użytkownikom danych osobowych,
2. Zabezpieczenie i kontrolowanie prawidłowości przebiegu czynności serwisowych sprzętu komputerowego oraz systemów informatycznych,
3. Pozbawianie zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie urządzeń lub nośników, które przeznaczone są do likwidacji,
4. Instalowanie zabezpieczeń w systemach informatycznych,
5. Wyrejestrowywanie i rejestrowanie z systemu użytkowników w czasie instalowania oraz modyfikacji systemu,
6. Przydzielanie uprawnień do poszczególnych systemów,
7. Wykonywanie kopii awaryjnych danych z serwera, właściwe przechowywanie nośników, sprawdzanie poprawności zapisu oraz ich likwidowanie,
8. Dokonywanie wyboru lub migracji do technologii minimalizującej zagrożenia uzyskania dostępu do sieci osobom nieupoważnionym,
9. Nadzorowanie procesu monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych,
10. Czuwanie nad właściwym eksploatowaniem podległych im systemów informatycznych,
11. Stwarzanie właściwych warunków organizacyjno-technicznych gwarantujących bezpieczeństwo podległych im systemów informatycznych,
12. Nadzorowanie właściwej lokalizacji sprzętu komputerowego, tj. ustawiania monitorów i drukarek uniemożliwiającego wgląd w dane osobowe osobom nieupoważnionym lub kradzież wymiennych nośników danych,
13. Nadawanie haseł dostępu użytkownikom oraz ustawianie uprawnień w podległych im systemach
14. Pozbawianie zapisu danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych,
15. Prowadzenie, uaktualnianie na bieżąco danych dotyczących:
    a) listy użytkowników danych osobowych wraz z przydzielonymi im uprawnieniami do poszczególnych funkcji systemu,
    b) lokalizacji pomieszczeń, w których te dane są przetwarzane, w przypadku jakichkolwiek zmian tych danych,
    c) rodzaju systemów informatycznych funkcjonujących w zakresie ich działania,
    d) czynności serwisowych wykonywanych w podległych systemach informatycznych,
    e) zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wykrytych wirusów, koni trojańskich itp. oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania.