

Zarządzenie Nr SK.0050.83.2015
Wójta Gminy Świerzno
z dnia 9 września 2015 r.

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

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

§ 1.1. Wyznaczam Panią Magdaleną Kłobucką na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy Świerzno. Zakres działania ABI stanowi załącznik Nr 1 do niniejszego zarządzenia.

2. Odwołuję Panią Izabelę Piasecką-Gajlun z funkcji Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Świerzno.

3. Wyznaczam Pana Dawida Mitłosza na Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Świerzno. Zakres działania ASI stanowi załącznik Nr 2 do niniejszego zarządzenia.

§ 2. Traci moc zarządzenie SK.0050.22.2015 Wójta Gminy Świerzno z dnia 16 kwietnia 2015 r. w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Gminy Świerzno.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.


WÓJT
Krzysztof Atras

Zakres działania Administratora Bezpieczeństwa Informacji (ABI)

Stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabranie przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem.

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) przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych,
- 6) kontrola nad danymi osobowymi wprowadzonymi do zbiorów (przez kogo zostały wprowadzone, komu są przekazywane),
- 7) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń,
- 8) nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,
- 9) nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych,
- 10) monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji uprawniony jest do:

- 1) wydawania poleceń wszystkim pracownikom Urzędu Gminy Świerzno w zakresie związanym ze wdrożeniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji,
- 2) rozstrzygania sporów dotyczących stosowania i interpretacji wymagań zawartych w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz wydawania wiążących decyzji w tym zakresie,
- 3) dostępu do wszystkich dokumentów występujących w Urzędzie Gminy Świerzno, których treść może być istotna z punktu widzenia funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji,
- 4) uzyskania wyjaśnień od pracowników w zakresie realizowanych działań w ramach Systemu Zarządzania Bezpieczeństwem Informacji,
- 5) podejmowania decyzji w kwestiach bezpieczeństwa Informacji, w zakresie nierodzącym zobowiązań finansowych, w szczególności w zakresie współpracy Urzędu Gminy Świerzno z zewnętrznymi jednostkami organizacyjnymi.

WOJCI
Przysztof Atras

Zakres działania Administratora Systemu Informatycznego (ASI)

Administrator Systemu Informatycznego, w zakresie zadań wykonywanych dla zapewnienia systemom bezpieczeństwa, zgodnego z celami i metodologią wdrożonej polityki bezpieczeństwa informacji, współpracuje bezpośrednio z Administratorem Bezpieczeństwa Informacji (ABI).

Do zadań Administratora Systemu Informatycznego należy:

- 1) formułowanie, w uzgodnieniu z administratorem danych i/lub osobami, do których administrator delegował zarządzanie uprawnieniami oraz ABI, sposobu określania uprawnień w systemach informatycznych,
- 2) realizacja decyzji Administratora Danych Osobowych (/innych) odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT Urzędu tj.:
 - a) tworzenie kont użytkowników w systemach informatycznych,
 - b) przypisywanie, do kont, startowych haseł uwierzytelniających użytkowników tych kont,
 - c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
 - d) resetowanie utraconych haseł,
 - e) usuwanie kont i uprawnień dla kont osób które zakończyły pracę w Urzędzie,
 - f) dostarczanie ABI informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowoprogramowych,
- 3) planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie Gminy,
- 4) planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych,
- 5) automatyzacja zadań konserwacyjnych w systemie – w tym wykonywania kopii zapasowych oprogramowania i danych,
- 6) monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników,
- 7) monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych,
- 8) zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych,

- 9) systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego,
- 10) zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki,
- 11) rozwiązywanie, samodzielnie i we współpracy z pozostałym personelem IT, problemów towarzyszących eksploatacji systemów informatycznych,
- 12) przygotowywanie, we współpracy z ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji,
- 13) prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT,
- 14) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
- 15) nadzór nad czynnościami związanymi z prowadzeniem systemu w zakresie obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywanych procedur uaktualniania systemów antywirusowych i ich konfiguracji,
- 16) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych,
- 17) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami sprzętu IT systemów informatycznych aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe,
- 18) prowadzenie ewidencji sprzętu komputerowego.


WOJT
Krzysztof Atras