

**Zarządzenie Nr WG.0050.115.2014
Wójta Gminy Ożarówce**

z dnia 21 lipca 2014 roku

w sprawie wyznaczenia i określenia zadań Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Gminy Ożarówce

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (j.t. Dz. U. z 2013r., poz.594 z późn. zm.), w związku z art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. Dz. U. z 2002r., Nr 101, poz. 926 z późn. zm.)

zarządzam, co następuje:

§ 1.

1. Wyznaczam Panią _____ na Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Ożarówce.
2. Ustalam zakres zadań i uprawnień Administratora Bezpieczeństwa Informacji, stanowiący załącznik nr 1 do niniejszego zarządzenia.

§ 2.

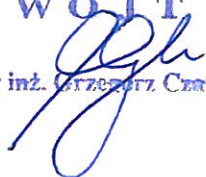
1. Wyznaczam Pana Zbigniewa Urbańczyka na Administratora Systemu Informatycznego w Urzędzie Gminy Ożarówce.
2. Ustalam zakres zadań Administratora Systemu Informatycznego, stanowiący załącznik nr 2 do niniejszego zarządzenia.

§ 3.

Wykonaniem zarządzenia powierzam Sekretarzowi Gminy Ożarówce.

§ 4.

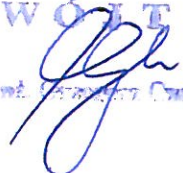
Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

mgr inż. Grzegorz Czarna

**Załącznik Nr 1
do Zarządzenia Nr WG.0050.115.2014
Wójta Gminy Ożarówce
z dnia 21 lipca 2014 roku**

**Zakres zadań i uprawnienia Administratora Bezpieczeństwa Informacji
w Urzędzie Gminy Ożarówce**

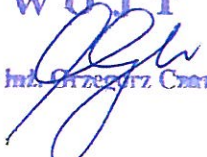
1. Administrator Bezpieczeństwa Informacji zwany dalej ABI podlega bezpośrednio Wójtowi Gminy Ożarówce.
2. Celem działania ABI jest nadzorowanie i kontrolowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w Urzędzie Gminy Ożarówce, a w szczególności nadzorowanie i kontrolowanie:
 - 1) stosowania środków technicznych i przedsięwzięć organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednich do zagrożeń oraz kategorii danych,
 - 2) zabezpieczenia danych osobowych przed udostępnieniem osobom nieupoważnionym lub zabranieniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem,
 - 3) przetwarzania danych osobowych zgodnie z przepisami w/w ustawy.
3. ABI realizując swoje zadania współpracuje z Administratorem Systemu Informatycznego (ASI). Do szczegółowych czynności ABI należy:
 - 1) nadzorowanie i kontrolowanie przestrzegania zasad:
 - a) przetwarzania danych osobowych przez użytkowników zgodnie z zakresem nadanego im upoważnienia,
 - b) stosowania przez użytkowników zasad przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania, zmieniania, udostępniania i ich usuwania,
 - c) ochrony obszarów przetwarzania danych w zakresie adekwatności stosowanych zabezpieczeń i możliwości wystąpienia w nich zagrożeń,
 - d) wyposażenia oraz zabezpieczenia pomieszczeń, w których przechowuje się dane sensytywne i kopie zapasowe zbiorów,
 - e) rejestracji zbiorów w Biurze Generalnego Inspektora Ochrony Danych Osobowych (GIODO) lub zmian przetwarzania danych osobowych,
 - f) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji upoważnień,
 - 2) realizowanie zadań w zakresie:
 - a) rozpatrywania skarg i wniosków dotyczących przetwarzania i ochrony danych,
 - b) tworzenia projektów zarządzeń, instrukcji i wytycznych Administratora Danych Osobowych,
 - c) przygotowywania informacji w zakresie rejestracji zbiorów w GIODO lub zmian w przetwarzaniu danych,
 - d) wyjaśniania i dokumentowania przypadków naruszania zasad przetwarzania i ochrony danych osobowych,
 - e) organizowania szkoleń z zakresu przetwarzania i ochrony danych osobowych,
 - f) odnotowywania i dokumentowania zmian w lokalizacjach obszarów przetwarzania danych,
 - g) wykonywania okresowych analiz zagrożeń bezpieczeństwa i ocen stanu ochrony danych osobowych przetwarzanych w obszarach.
4. Wykonując swoje czynności ABI działa w imieniu Administratora Danych Osobowych i posiada uprawnienia do:
 - 1) wskazywania zastosowania odpowiednich zabezpieczeń technicznych i wykonywania czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony danych,
 - 2) wnioskowania o ograniczenie zakresu przetwarzania danych osobowych użytkownikom, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych,
 - 3) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie kontroli i dostosowania ochrony danych do stanu zgodnego z przepisami prawa,
 - 4) zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych.

WÓJT

mgr hab. inż. Andrzej Ożarówce

Załącznik Nr 2
do Zarządzenia Nr WG.0050.115.2014
Wójta Gminy Ożarówice
z dnia 21 lipca 2014 roku

Zakres zadań Administratora Systemu Informatycznego w Urzędzie Gminy Ożarówice

1. Administrator Systemu Informatycznego zwany dalej ASI, wykonuje zadania w zakresie niniejszego zarządzenia, a w szczególności:
 - 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 uszkodzanie 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) wykonywanie poleceń Administratora Bezpieczeństwa Informacji w zakresie zarządzania podległymi systemami informatycznymi,
 - 11) czuwanie nad właściwym eksploataowaniem podległych im systemów informatycznych,
 - 12) stwarzanie właściwych warunków organizacyjno-technicznych gwarantujących bezpieczeństwo podległych im systemów informatycznych,
 - 13) nadzorowanie właściwej lokalizacji sprzętu komputerowego, tj. ustawiania monitorów i drukarek uniemożliwiającego wgląd w dane osobowe osobom nieupoważnionym lub kradzież wymiennych nośników danych,
 - 4) występowanie do Administratora Danych Osobowych z wnioskiem o upoważnienie pracowników do przetwarzania danych osobowych,
 - 15) nadawanie haseł dostępu użytkownikom oraz ustawianie uprawnień w podległych im systemach,
 - 16) pozbawianie zapisu danych osobowych z nośników, które przeznaczone są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych,
 - 17) prowadzenie, uaktualnianie na bieżąco oraz przesyłanie Administratorowi Bezpieczeństwa Informacji 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,
 - 18) zgłaszanie Administratorowi Bezpieczeństwa Informacji potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych.

WÓJTA

mgr inż. Grzegorz Czerniak

