Załącznik nr 3
do Zarządzenia nr 7/2013
Przewodniczącego Zarządu Związku Gmin Krajny w Złotowie
z dnia 21sierpnia 2013r.

Instrukcja bezpieczeństwa użytkownika systemu informatycznego Związku Gmin Krajny w Złotowie

1) Dostęp do systemu informatycznego może uzyskać tylko osoba zarejestrowana w tym systemie przez administratora po podaniu identyfikatora i hasła. Dobór właściwie zbudowanych haseł i czasu okresu ich ważności stanowi jedną z najważniejszych zasad ochrony systemu informatycznego przed intruzami. Kryteria doboru haseł i czasu okres ich obowiązywania ustala administrator za pomocą oprogramowania systemowego.

2) Wszystkie komputery (serwery i stacje robocze) ZGK są wyposażone w oprogramowanie antywirusowe. Zabrania się wyłączania tego oprogramowania. Dane zawarte na nośnikach zewnętrznych (np. pamięci masowe USB) muszą być sprawdzone przez program antywirusowy przed wprowadzeniem do systemu. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z administratorem sieci lokalnej.

3) Użytkownicy stacji roboczych nie mają prawa dokonywać samodzielnie jakichkolwiek instalacji oprogramowania zarówno na stacjach roboczych, jak i na serwerach sieci. Za instalację i konfigurowanie oprogramowania odpowiadają wyznaczone osoby zajmujące się administracją. Administratorzy są odpowiedzialni za instalację uaktualnień i oprogramowania.

4) Administrator przygotowuje, a przełożony odpowiedniego szczebla zatwierdza listę oprogramowania dopuszczoną do użytkowania na stacjach roboczych w zależności od typu prac na nich wykonywanych.

5) Zabrania się wszelkich prac z wykorzystaniem oprogramowania, na które użytkownik nie ma ważnej licencji (zakaz nie dotyczy programów, na użytkowanie, których licencja nie jest wymagana) lub niewiadomego pochodzenia.

6) Użytkownicy zobowiązani są do zachowania szczególnej ostrożności przy pracy z pocztą elektroniczną. W przypadku jakichkolwiek wątpliwości, szczególnie w przypadku załączników poczty elektronicznej, należy przed uruchomieniem skontaktować się z administratorem.

7) Przy wprowadzaniu do systemu nowych programów lub danych zawsze należy kierować się zasadą ograniczonego zaufania.

Zatwierdzam powyższej instrukcji pod względem formalnoprawnym. Każda strona została podpisana.

Radosław Kilar

8) Za sporządzanie kopii bezpieczeństwa informacji znajdujących się na serwerach odpowiada administrator. Wykonywanie kopii bezpieczeństwa danych znajdujących się na stacjach roboczych należy do obowiązków użytkowników. Dopuszcza się wykonywanie kopii bezpieczeństwa przy wykorzystaniu serwera plików ADMIN. Zaleca się zapisywanie istotnych zbiorów danych na udostępnionych przez administratora dyskach sieciowych.

9) Bezpieczeństwo na styku z siecią INTERNET zapewniają systemy firewall. Zabrania się dokonywania połączeń modemowych z sieci lokalnej do sieci INTERNET z pominięciem oprogramowania Firewall. Jeżeli komputer przenośny został, podczas pracy w terenie, podłączony do sieci INTERNET, to przed podłączeniem do sieci lokalnej cały jego dysk twardy musi być sprawdzony zaktualizowanym programem antywirusowym.

10) Wykonywanie prac pozasłużbowych dopuszcza się w wyjątkowych przypadkach - za zgodą przełożonych.

11) Zabrania się pozostawienia sprzętu komputerowego niezabezpieczonego przed dostępem osób nieuprawnionych, bez nadzoru osoby odpowiedzialnej za jego użytkowanie.

RADCA PRAWNY
BdP - 209
Radosław Kilar