

Zarządzenie Nr 1/2015
Wójta Gminy Biskupiec
z dnia 8 stycznia 2015 roku

w sprawie powołania Administratora Systemów Informatycznych

Na podstawie art. 31 oraz art. 33 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Tekst jednolity: Dz. U. z 2013r. poz. 594 z późn. zm) w związku z art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Tekst jednolity Dz. U. z 2014r. poz.1182)

ustanawiam

z dniem 08.01.2015 roku

Pana Łukasza Foj

ADMINISTRATOREM SYSTEMÓW INFORMATYCZNYCH
w Urzędzie Gminy Biskupiec

Zakres czynności dla Administratora Systemów Informatycznych stanowi załącznik nr 1 do niniejszego zarządzenia


WÓJTA
mgr inż. Arkadiusz Dobek

Załącznik Nr 1
do Zarządzenia Nr 1/2015
Wójta Gminy Biskupiec
z dnia 8 stycznia 2015r.

Zakres czynności Administratora Systemów Informatycznych
w Urzędzie Gminy Biskupiec

1. Nadawanie identyfikatorów użytkownikom danych osobowych,
2. Zabezpieczenie i kontrolowanie prawidłowości przebiegu czynności serwisowych sprzętu komputerowego oraz systemów informatycznych,
3. Pozbawienie zapisu danych osobowych lub uszkodzenie 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 eksploataowaniem 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 przeznaczone 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,