Załącznik Nr 2
do Zarządzenia Nr 28/OR/09
Wójta Gminy Łodygowice
z dnia 20.04.2009r

INSTRUKCJA
zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

Niniejsza instrukcja reguluje sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Urzędzie Gminy Łodygowice uwzględniający wymogi określone w § 11 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r, Nr 100, poz. 1024).

I. Bezpieczeństwo systemu informatycznego

1. Każdy użytkownik systemu informatycznego, służącego do przetwarzania danych osobowych posiada indywidualny identyfikator i hasło, które umożliwiają mu na pracę w systemie.
2. Identyfikator użytkownika:
    a. nadaje Administrator Bezpieczeństwa Informacji na wniosek bezpośredniego przełożonego pracownika zgodnie z instrukcją systemu informatycznego i wpisuje do ewidencji osób zatrudnionych przy przetwarzaniu danych wraz z imieniem i nazwiskiem użytkownika oraz rejestruje w systemie informatycznym,
    b. pozostaje niezmieniony przez cały czas pracy użytkownika, a po jej zakończeniu nie może być przydzielony innemu użytkownikowi systemu,
    c. w przypadku utraty przez pracownika uprawnień do dostępu do danych osobowych – na wniosek przełożonego pracownika – Administrator Bezpieczeństwa Informacji wyrejestrowuje użytkownika z systemu informatycznego.
3. Hasło użytkownika:
    a. wymagane do pierwszego logowania się w systemie przydzielane jest przez Administratora Bezpieczeństwa Informacji, użytkownik przy pierwszym logowaniu zobowiązany jest do jego zmiany,
    b. jest znane tylko użytkownikowi i powinno być trzymane w tajemnicy również po upływie jego ważności,
    c. powinno być zmieniane nie rzadziej niż raz na miesiąc przez użytkownika systemu lub jeżeli system informatyczny przewiduje taką możliwość zgodnie z instrukcją eksploatacyjną systemu,
    d. powinno składać się co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
4. Hasła Administratora przechowywane są w zamkniętej kopercie w sejfie, do którego ma dostęp Wójt oraz Administrator. W przypadku użycia awaryjnego tych haseł konieczny jest wpis do „Dziennika haseł".
5. Za prawidłowe prowadzenie zabezpieczenia systemów oraz pełną jego dokumentację merytorycznie odpowiada Administrator Bezpieczeństwa Informacji.

II. Kopie bezpieczeństwa

1. Kopie awaryjne systemów tworzy się na komputerowych nośnikach informacji w trybie i terminach określonych w instrukcjach eksploatacyjnych systemów.
2. Kopie awaryjne serwera wykonuje ABI lub osoba przez niego upoważniona, kopie na stacjach roboczych wykonuje użytkownik danego stanowiska.

3. Kopie awaryjne winne być przechowywane w miejscach odpowiednio zabezpieczonych (sejfy, szafy pancerne itp.) – najlepiej poza pomieszczeniami, gdzie przetwarzane są systemy informatyczne.
4. Raz na 3 miesiące należy sprawdzić kopie awaryjne pod kątem ich przydatności do odtworzenia danych.
5. Po ustaniu użyteczności kopii awaryjnej użytkownik systemu zobowiązany jest przekazać kopię Administratorowi Bezpieczeństwa Informacji, który trwale usunie z niej dane.

III. Przeglądy i konserwacja

1. Komputerowe nośniki informacji zawierające dane osobowe przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych lub uszkadza się je w sposób uniemożliwiający ich odczytanie.
2. W przypadku przekazywania komputera z nośnikiem danych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonywać naprawy w obecności osoby upoważnionej przez ABI.
3. Komputery i urządzenia służące do przetwarzania danych osobowych należy wyposażyć na wypadek awarii zasilania w zasilacze awaryjne.
4. Do ochrony antywirusowej stosuje się programy antywirusowe zainstalowane na każdym komputerze.
5. Skanowanie stacji roboczych odbywa się automatycznie po ich uruchomieniu.
6. Korzystanie z zewnętrznych nośników informacji (dyskietek, dysków wymiennych, płyt CD, poczty elektronicznej, itp.) może mieć miejsce wyłącznie po sprawdzeniu programem antywirusowym.

IV. Komputerowe stanowisko pracy

1. ABI w porozumieniu z kierownikiem jednostki ustala czas pracy użytkownikom systemu. Na pracę poza godzinami funkcjonowania urzędu użytkownik systemu musi uzyskać zgodę kierownika oraz dokonać wpisu do rejestru.
2. Osoby, których dane są przetwarzane powinny mieć możliwość zapoznania się z tymi danymi oraz być poinformowane o przysługującym im prawie wynikającym z ustawy o ochronie danych osobowych.
3. W pomieszczeniach gdzie przyjmowani są klienci, monitory powinny być tak ustawione, aby uniemożliwić osobom niepowołanym wgląd w dane.
4. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu lub po 2 minutach powinien uruchomić się wygaszasz ekranu zabezpieczony hasłem.
5. Użytkownikowi nie wolno instalować oprogramowania bez zgody ABI.

V. Serwery.

1. Serwery zlokalizowane są w pomieszczeniu zabezpieczonym i klimatyzowanym.
2. W serwerowi mogą przebywać tylko osoby upoważnione przez ABI.
3. Osoby dokonujące napraw, konserwacji i instalacji programów bądź urządzeń mogą przebywać tylko w obecności ABI lub osób przez niego upoważnionych.

VI. Tryb postępowania w sytuacji naruszenia ochrony danych osobowych.

1. Każdy pracownik, który stwierdzi naruszenie ochrony danych osobowych w zbiorach informatycznych, informuje o tym fakcie swojego przełożonego oraz ABI.
2. ABI doraźnie usuwa przyczynę naruszenia systemu informatycznego oraz informuje o zaistniałym zdarzeniu kierownika jednostki.
3. Kierownik jednostki wdraża postępowanie wyjaśniające.