Załącznik nr 2
do Zarządzenia Nr 62/2011
Burmistrza Gminy Czempiń
z dnia 30 maja 2011r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY W CZEMPINIU

Rozdział I
Postanowienia ogólne

§1.

Instrukcja zarządzania systemem informatycznym Urzędu Gminy w Czempiniu, zwana dalej „Instrukcją", określa sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji oraz postępowania w sytuacjach naruszenia ochrony danych osobowych w Urzędzie. Jest dokumentem wewnętrznym wydanym przez Administratora Danych osobowych – Burmistrza Gminy Czempiń i ma zastosowanie do przetwarzania danych osobowych w systemach informatycznych urzędu w celu bezpiecznego ich wykorzystywania.

Rozdział II
Procedury nadawania i zmiany uprawnień do przetwarzania danych

§2.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych zobowiązany jest zapoznać się z:
   - ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz.926 z późn. Zm.),
   - Polityką bezpieczeństwa zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Czempiniu
   - Instrukcją Zarządzania Systemu Informatycznym Urzędu Gminy w Czempiniu.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik nr 1 do Instrukcji.
3. Administrator Bezpieczeństwa informacji przyznaje upoważnienie w zakresie dostępu do systemu informatycznego na podstawie pisemnego wniosku Administratora Danych określającego zakres uprawnień pracownika. Wzór wniosku o nadanie uprawnień w systemie informatycznym określa Załącznik nr 2 do Instrukcji. Wzór upoważnienia do przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy w Czempiniu stanowi załącznik nr 3 do Instrukcji.
4. Jedynie prawidłowo wypełniony wniosek o nadanie uprawnień w systemie oraz zmianę tych uprawnień jest podstawą rejestracji uprawnień w systemie.
5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji (o ile system na to pozwala).
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane

będą jako naruszenie podstawowych obowiązków pracowniczych.

9. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
10. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
11. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielony w sieci lokalnej.
12. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
13. Pracownicy zatrudnieni przy przetwarzaniu danych osobowych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
14. Identyfikator osoby, która utraciła uprawnienia dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło dostępu.
15. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników ich uprawnień w systemie informatycznym.
16. Rejestr powinien zawierać:
    - imię i nazwisko użytkownika systemów informatycznych,
    - rodzaj uprawnienia,
    - datę nadania uprawnienia,
    - datę odebrania uprawnienia,
    - przyczynę odebrania uprawnienia,
    - podpis Administratora Bezpieczeństwa Informacji.

Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników

Rozdział III
Zasady posługiwania się hasłami

§3.

1. Bezpośredni dostęp do danych osobowych przetwarzanych systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być znane tylko użytkownikowi.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji kiedy zachodzi podejrzenie, ze ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
8. Zmiany hasła nie wolno zlecać innym osobom.
9. W systemach, które umożliwiają opcje zapamiętywania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia,
10. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie zamykanej na klucz szafie metalowej, do której dostęp mają:
    - Administrator Bezpieczeństwa Informacji,
    - Kierownik Urzędu lub osoba przez niego wyznaczona

Rozdział IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§4.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwacji należy wykonać opcje wylogowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.

Rozdział V
Procedura tworzenia zabezpieczeń

§5.

1. Kopie zapasowe tworzy się poprzez zapisanie danych na dodatkowych nośnikach w zależności od potrzeb programu.
2. Kopie zapasowe są sprawdzane pod kątem dalszej ich przydatności do odtworzenia danych w przypadku awarii systemu raz na sześć miesięcy.
3. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
4. Zdezaktualizowane i uszkodzone kopie zapasowe należy mechanicznie zniszczyć w sposób uniemożliwiający ich ponowne użycie.
5. Urządzenia systemy informatyczne służące do przetwarzania danych osobowych, zabezpiecza się przed utratą danych w przypadku awarii zasilania poprzez zainstalowanie zasilaczy awaryjnych.

Rozdział VI
Sposób i miejsce przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków

§6.

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   - likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   - przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   - naprawy- pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie lub naprawia się pod nadzorem osoby upoważnionej przez Administratora Danych.
2. Dane osobowe w postaci elektronicznej zapisane na nośnikach nie są wynoszone poza siedzibę Urzędu.
3. Wydruki zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
4. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie np. za pomocą niszczarki.

Rozdział VII
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest dostęp lub uszkodzenie systemu informatycznego

§7.

1. Na każdym stanowisku komputerowym podłączanym do sieci publicznej musi być zainstalowane oprogramowanie antywirusowe pracujące trybie monitora.
2. Każdy e-mail musi być sprawdzony pod katem występowania wirusów. Sprawdzenia dokonuje użytkownik, który pocztę otrzymał.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się samowolnego instalowania programów komputerowych.
7. Zabrania się korzystania z programów P2P(peer-to-peer): Mule, kazaa itp., grup dyskusyjnych oraz czatów.
8. Administrator Bezpieczeństwa Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach minimum, co sześć miesięcy.
9. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
10. W przypadku wykrycia wirusa komputerowego sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto.

Rozdział VIII
Zasady i sposób odnotowywania w systemie informacji o udostępnianiu danych osobowych

§8.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną .
4. Udostępnianie danych osobowych może nastąpić wyłącznie na pisemny wniosek.
5. Pracownicy przetwarzający dane osobowe prowadzą rejestry udostępnionych danych osobowych zawierające, co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję, dla której dane udostępniono.

Rozdział IX
Procedury wykonywania przeglądów i konserwacji systemu

§9.

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu lub w zależności od potrzeb.
2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie

usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

3. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

Rozdział X
Podłączenie do sieci publicznej

§10.

Podłączenie lokalnej sieci komputerowej Urzędu z siecią publiczną jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych oraz oprogramowania antywirusowego.

Rozdział XI
Sposób postępowania w sytuacji stwierdzenia naruszenia ochrony danych osobowych

§11.

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub bezpośredniego przełożonego lub Administratora Danych,
2. Należy niezwłocznie zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych.
3. Pracownik podejmuje działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia – o ile czynności te nie spowodują przekroczenia uprawnień pracownika.
4. Zabezpiecza się dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa danych osobowych.
5. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona podejmuje czynności wyjaśniające mające na celu ustalenie:
   - przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych,
   - osób winnych naruszenia bezpieczeństwa danych osobowych,
   - skutków naruszenia,
6. Administrator Bezpieczeństwa Informacji zobowiązany jest do powiadomienia o zaistniałej sytuacji Administratora Danych, który podejmuje decyzje o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu, ponownym przystąpieniem do pracy oraz o powiadomieniu organów ścigania.
7. Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego co najmniej:
   - datę i miejsce wystąpienia naruszenia,
   - zakres ujawnionych danych,
   - przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy,
   - sposób rozwiązywania problemu,
   - przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

   Raport ten Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych.

Rozdział XII
Znajomość Instrukcji

§12.

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym.

Załącznik nr 1
do Instrukcji zarządzania
systemem informatycznym
Urzędu Gminy w Czempiniu

Czempiń, dnia.....

.....
(nazwisko i imię)

.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, iż w związku z wykonywanymi obowiązkami służbowymi, przetwarzam lub mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym zapoznałem(am) się z:

1. Ustawą z dnia 29 sierpnia 1997 r. O ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. Zm.),
2. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 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. Nr 100, poz. 1024),
3. Dokumentem „Polityka bezpieczeństwa zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Czempiniu".
4. Dokumentem „Instrukcja Zarządzania Systemem Informatycznym Urzędu Gminy w Czempiniu"

Jednocześnie zobowiązuję się do zachowania w tajemnicy, także po ustaniu stosunku pracy wszelkich informacji związanych z przetwarzaniem danych osobowych.

.....

(podpis pracownika)

Załącznik nr 2
Do Instrukcji zarządzania
systemem informatycznym
Urzędu Gminy W Czempiniu

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Nowy użytkownik ☐	Modyfikacja systemie ☐	Odebranie uprawnień w systemie informatycznym ☐

1. Imię i nazwisko użytkownika - .....
2. Stanowisko pracy -.....
3. Opis zakresu uprawnień użytkownika w systemie informatycznym:

.....

.....

.....

.....

Data wystawienia

Podpis bezpośredniego przełożonego użytkownika

.....

Podpis Administratora Danych

.....

Załącznik nr 3
Do Instrukcji zarządzania
systemem informatycznym
Urzędu Gminy W Czempiniu

Czempiń, dnia .....

.....
(pieczęć jednostki organizacyjnej)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. O ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926 z późn. Zm.) upoważniam:

.....
(imię i nazwisko)

zatrudnionego(ną) na stanowisku
.....
do przetwarzania danych osobowych oraz obsługo systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w Urzędzie Gminy w Czempiniu w zakresie …….

.....
(podpis i pieczęć administratora danych)