Załącznik nr 3 do Zarządzenia Nr 31/2011
Wójta Gminy Ostrowice
z dnia 20 lipca 2011 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY OSTROWICE

§ 1. Definicje:

1) **urząd –** należy przez to rozumieć Urząd Gminy Ostrowice;

2) **administrator danych** – Wójt Gminy Ostrowice;

3) **administrator bezpieczeństwa informacji (ABI)** – pracownik urzędu lub inna osoba wyznaczona do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

4) **administrator systemu informatycznego (ASI)** – to osoba odpowiedzialna za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony;

5) **użytkownik systemu** – to osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno prawnej, osoba odbywająca staż w urzędzie, wolontariusz;

6) **identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

7) **hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

8) **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

9) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

10) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom.

§ 2. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym zwanym dalej systemem oraz wskazanie osoby odpowiedzialnej za te czynności:

1) uprawnienia do przetwarzania danych osobowych nadawane są przez administratora danych na wniosek kierownika właściwej komórki organizacyjnej lub pracownika zatrudnionego na samodzielnym stanowisku. Uprawnienia dotyczą zarówno danych osobowych gromadzonych w systemie informatycznym, jak również w tradycyjnych zbiorach papierowych. Wzór upoważnienia stanowi ***załącznik Nr 1*** do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice;
2) zgoda na pracę w systemie informatycznym jest wymagana także dla użytkowników, którzy nie przetwarzają danych osobowych;
3) wprowadza się rejestr upoważnień i osób zatrudnionych przy przetwarzaniu danych osobowych oraz osób pracujących w systemie, którego wzór stanowi ***załącznik Nr 2*** do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice;
4) rejestr prowadzony jest przez administratora bezpieczeństwa informacji w postaci elektronicznej oraz papierowej;
5) uprawnienia o których mowa w pkt 1 wydawane są na czas zatrudnienia w Urzędzie Gminy Ostrowice;
6) użytkowników systemu tworzy oraz usuwa za zgodą administratora danych, administratora bezpieczeństwa informacji lub osoby przez niego upoważnionej;
7) osoby, które zostały upoważnione do przetwarzania danych osobowych, są obowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia;
8) każdy pracownik Urzędu Gminy Ostrowice podpisze oświadczenie, którego wzór stanowi ***załącznik Nr 3*** do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice.

§ 3. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem:

1) każdy użytkownik systemu dopuszczony do pracy przy przetwarzaniu danych osobowych powinien posiadać odrębny, jednoznacznie identyfikujący pracownika login;
2) wprowadza się obowiązek uwierzytelnienia własnego loginu poprzez podanie hasła;
3) zmianę hasła należy dokonywać nie rzadziej niż co 30 dni;
4) hasło składa się co najmniej z 8 znaków, musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;

5) początkowe hasło dostępu ustala się z administratorem bezpieczeństwa informacji, a następnie użytkownik systemu samodzielnie zmienia je przy użyciu odpowiednich narzędzi informatycznych;

6) dane osobowe gromadzone są wyłącznie na macierzy dyskowej. Zabrania się gromadzenia danych osobowych na innych nośnikach danych;

7) w uzasadnionych przypadkach, za zgodą administratora bezpieczeństwa informacji, dane osobowe można przetwarzać poza serwerem;

8) tworzy się rejestr zewnętrznych nośników informacji na których przetwarzane są dane osobowe;

9) rejestr o którym mowa w pkt 8 prowadzi administrator bezpieczeństwa informacji;

10) za zabezpieczenie danych osobowych przechowywanych w tradycyjnych rejestrach papierowych odpowiadają pracownicy zatrudnieni na samodzielnych stanowiskach i kierownicy właściwych komórek organizacyjnych.

§ 4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

1) logowanie do systemu następuje po podaniu identyfikatora oraz hasła dostępu;

2) użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień;

3) zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu;

4) zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3;

5) zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.

§ 5. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Archiwizacja zbiorów danych osobowych znajdujących się na macierzy dyskowej wykonywana jest co najmniej jeden raz w tygodniu i zapisywana na zewnętrzne elektroniczne nośniki informacji;

2. Kopie danych o których mowa w ust. 1 wykonuje administrator systemu informatycznego lub osoba przez niego upoważniona.

§ 6. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz kopii zapasowych:

1) dane o których mowa w § 5 ust. 1 zapisywane są na macierze dyskowe;

2) nośniki z danymi przechowywane są w Urzędzie Gminy Ostrowice w pokoju nr 1, w szafie do której wyłączny dostęp ma administrator bezpieczeństwa informacji, administrator systemu informatycznego lub osoba przez niego upoważniona;

3) kopie danych o których mowa w § 5 ust. 1 nadpisuje się w przypadku kończącej się wolnej przestrzeni dyskowej na macierzy;

4) urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się mechanicznie w sposób uniemożliwiający ich odczytanie,
   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
   c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych osobowych;

5) urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania danych zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

§ 7. Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:

1) system obejmuje się ochroną antywirusową polegającą na skanowaniu serwerów oraz stacji roboczych programem antywirusowym;

2) skanowanie serwerów wykonywane jest co najmniej raz w tygodniu przez administratora systemu informatycznego lub osobę przez niego upoważnioną;

3) skanowanie stacji roboczych wykonują ich użytkownicy;

4) użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, a także plików danych pobieranych z zasobów sieci Internet oraz otrzymanych w poczcie elektronicznej;

5) w celu zabezpieczenia systemu przed ingerencją z zewnątrz, systemy posiadają włączone ściany ogniowe;

6) przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej system jest chroniony zasilaczami awaryjnymi (UPS);

7) każda jednostka komputerowa jest zabezpieczona hasłem do BIOS-a.

§ 8. Informacje o odbiorcach, w rozumieniu art. 7 pkt. 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia:

1) tworzy się centralną ewidencję udostępniania danych prowadzoną w formie elektronicznej oraz papierowej, która w szczególności powinna zawierać co najmniej następujące pola: nazwa odbiorcy, data udostępnienia, zakres udostępnienia;

2) ewidencję, o której mowa w pkt 1 prowadzi administrator bezpieczeństwa informacji;

3) kierownicy komórek organizacyjnych pracownicy pracujący na samodzielnych stanowiskach są zobowiązani do tego, aby o fakcie udostępniania danych informować administratora bezpieczeństwa informacji, który dokonuje odpowiednich zapisów w ewidencji o której mowa w pkt 1.

§ 9. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1) przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez administratora danych;

2) czynności określone w pkt 1 mogą być wykonywane w obecności osoby upoważnionej do przetwarzania danych osobowych;

3) tworzy się ewidencję osób upoważnionych do wykonywania prac o których mowa w pkt 1;

4) ewidencję o której mowa w pkt 3 prowadzi w formie elektronicznej i papierowej administrator bezpieczeństwa informacji. Ewidencja ta zawiera następujące pola: imię i nazwisko, data, zakres wykonywanej czynności.

§ 10. Szczegółowe zasady korzystania ze sprzętu komputerowego i systemów informatycznych, poczty elektronicznej oraz Internetu określa Regulamin Użytkownika Systemów Teleinformatycznych Urzędu Gminy Ostrowice, który stanowi *załącznik Nr 4* do Instrukcji zarządzania systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice.

Załącznik Nr 1 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice

Ostrowice, dnia ..... 20…. r.

U P O W A Ż N I E N I E Nr .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

upoważniam.....

zatrudnioną /-ego/ na stanowisku .....

do przetwarzania danych osobowych oraz obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice.

Niniejsze upoważnienie jest ważne na czas zatrudnienia w jednostce.

Administrator Danych
Wójt Gminy Ostrowice

Wacław Micewski

Załącznik Nr 2 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice

Rejestr upoważnień i osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Gminy Ostrowice.

Nr upoważ-nienia	Imię i nazwisko	Komórka organizacyjna	Data nadania upoważ-nienia	System
1/2012				
2/2012				
3/2012				
4/2012				
5/2012				

Załącznik Nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice

---
(imię i nazwisko pracownika)

(stanowisko)

(nazwa komórki organizacyjnej lub stanowiska)

O Ś W I A D C Z E N I E

1. Oświadczam, że znam treść:

   1) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.);
   2) rozporządzenia 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) Regulaminu Użytkownika Systemów Teleinformatycznych Urzędu Gminy Ostrowice.

Ostrowice, dnia ..... 20…… r.

..... ……..

(podpis pracownika) (podpis złożono w obecności)

Załącznik Nr 4 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ostrowice

REGULAMIN UŻYTKOWNIKA SYSTEMÓW TELEINFORMATYCZNYCH URZĘDU GMINY OSTROWICE

§ 1. Zasady korzystania ze sprzętu komputerowego i systemów informatycznych:

1) użytkownik zobowiązany jest do bezterminowego zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Pracodawcę na szkodę;

2) tworzenie kont w systemach, nadawanie, modyfikacja oraz usunięcie uprawnień, instalacja lub deinstalacja oprogramowania, grupowa instalacja lub deinstalacja, wydanie lub przekonfigurowanie sprzętu odbywa się na wniosek osoby zainteresowanej. Wnioski realizowane są przez Administratora Systemu Informatycznego;

3) sprzęt komputerowy oraz zainstalowane na nim oprogramowanie, jakie zostało oddane użytkownikowi w okresie jego pracy jest wykorzystywany tylko do celów służbowych;

4) użytkownik dba o powierzony mu sprzęt oraz chroni go przed szkodliwym wpływem warunków zewnętrznych;

5) użytkownik zabezpiecza w miarę posiadanych możliwości sprzęt przed kradzieżą;

6) hasła użytkowników do systemów podlegają następującym zasadom:
   a) hasło składa się z minimum 8 znaków, przy czym zawiera wielkie i małe litery, oraz cyfry lub znaki specjalne,
   b) hasło musi być zmieniane minimum co 30 dni,
   c) kolejne hasła muszą być różne,
   d) hasła należy przechowywać w sposób gwarantujący ich poufność,
   e) zabrania się udostępniania haseł innym osobom;

7) zabrania się tworzenia haseł na podstawie:
   a) cech i numerów osobistych (np. dat urodzenia, imion itp.),
   b) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
   c) identyfikatora użytkownika,
   d) innych haseł łatwych do odgadnięcia.

8) użytkownicy nie mogą udostępniać innym osobom indywidualnych identyfikatorów (nazwa użytkownika, token, karta inteligentna i inne dane umożliwiające uwierzytelnienie);

9) użytkownik zobowiązany jest przestrzegać zasady „czystego biurka" i „czystego ekranu". Stosowanie tych zasad sprowadza się do:

    a) schowania wszystkich dokumentów, nośników danych, związanych z informacjami chronionymi w miejsce niedostępne dla innych osób po zakończeniu pracy,
    b) odchodząc od stacji roboczej, użytkownik blokuje komputer uniemożliwiając zalogowanie się do systemu osobie nieuprawnionej,
    c) kończąc pracę użytkownik zamyka wszystkie aplikacje, wylogowuje się z systemu i wyłącza komputer;

10) zabrania się użytkownikom uruchamiać (w tym aplikacji przenośnych ang. portable) i instalować na sprzęcie służbowym jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonuje Administrator Systemu Informatycznego, na podstawie pisemnych wniosków;

11) zabrania się użytkownikom:

    a) omijania mechanizmów kontroli (np. używania serwerów proxy),
    b) testowania wdrożonych zabezpieczeń,
    c) skanowania urządzeń sieciowych, serwerów oraz stacji roboczych pod kątem badania świadczonych usług,
    d) wyłączania programów uruchamianych automatycznie przy starcie systemu,
    e) odinstalowania programów,
    f) przyłączania i użytkowania prywatnego sprzętu, w tym używania prywatnych nośników danych,
    g) podejmowania jakichkolwiek prób ingerencji w sprzęt komputerowy, poza czynnościami związanymi z codzienną eksploatacją;

12) ważne pliki należy przechowywać w wyznaczonych folderach na serwerach, które gwarantują bezpieczeństwo danych;

13) za bezpieczeństwo danych przechowywanych lokalnie na komputerze odpowiada użytkownik;

14) zabrania się przechowywania na sprzęcie służbowym gier oraz plików multimedialnych np. filmów, obrazów, dźwięków nie związanych z zadaniami służbowymi;

15) na sprzęcie komputerowym instaluje się oprogramowanie do ilościowej jak i jakościowej kontroli użytkowników, które stosuje się w celu okresowej kontroli wykorzystania sprzętu służbowego przez użytkowników;

16) w przypadku używania zewnętrznych nośników danych na stacji roboczej użytkownik wcześniej wykonuje skanowanie programem antywirusowym wszystkich danych na nośniku;

17) w przypadku gdy użytkownik wykryje zainfekowane dane niezależnie od źródła (np. strona internetowa, załącznik poczty elektronicznej, dane na nośniku) bezzwłocznie powiadamia o tym fakcie Administratora Systemu Informatycznego;

18) zabrania się użytkownikom samodzielnego przenoszenia i podłączania sprzętu teleinformatycznego między stanowiskami pracy. Czynności te wykonuje Administrator Systemu Informatycznego;

19) kończąc świadczenie pracy dla Pracodawcy, użytkownik ma obowiązek przekazać wszystkie dane (dokumenty papierowe, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi przełożonemu.

§ 2. Zasady korzystania z poczty elektronicznej:

1) nadzór i opiekę techniczną nad systemem poczty elektronicznej sprawuje Administrator Systemu Informatycznego. Użytkownik zobowiązany jest do sprawdzania własnej skrzynki poczty elektronicznej;

2) poczta elektroniczna jest wykorzystywana tylko do celów służbowych;

3) zabrania się rozsyłania m.in.:
   a) ogłoszeń komercyjnych,
   b) tzw. łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej),
   c) treści wulgarnych,
   d) materiałów erotycznych,
   e) treści niezgodnych z obowiązującymi przepisami prawa,
   f) treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowanie;

4) korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Pracodawcy;

5) pracodawca w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli skrzynek pocztowych użytkowników. O wynikach kontroli powinien być poinformowany użytkownik;

6) nie należy otwierać linków oraz załączników poczty elektronicznej ze źródeł niewiadomego pochodzenia;

7) w przypadku dostępu do poczty elektronicznej z sieci Internet należy przeczytać uważnie pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa i nigdy nie ignorować ostrzeżeń;

8) nie zaleca się logowania do systemów poczty elektronicznej z komputerów dostępnych publicznie (np. kafejki internetowe);

9) skrzynki pocztowe posiadają ograniczoną wielkość. Użytkownik zobowiązany jest do okresowej archiwizacji wiadomości.

§ 3. Zasady korzystania z Internetu:

1) Użytkownicy korzystają z dostępu do Internetu tylko w celach służbowych;

2) praca w sieci Internet nie może zagrażać bezpieczeństwu systemów informatycznych;

3) Pracodawca może wprowadzić kategoryzację stron internetowych oraz zablokować dostęp do wybranych kategorii;

4) Odblokowanie witryny internetowej może nastąpić na pisemny wniosek kierownika komórki organizacyjnej lub pracownika pracującego na samodzielnym stanowisku;

5) Zabrania się:

   a) wykorzystywania sieci Internet w sposób, który mógłby narazić Pracodawcę na utratę dobrego imienia,
   b) pobierania oprogramowania (w tym, w wersjach darmowych), nie związanego z wykonywanymi obowiązkami służbowymi,
   c) podłączania sieci Internet do fizycznie odseparowanych sieci,
   d) udostępniania łącza internetowego dostarczonego przez Pracodawcę innym osobom bez zgody Pracodawcy oraz Administratora Systemu Informatycznego,
   e) instalowania urządzeń udostępniających Internet na sprzęcie Pracodawcy bez zgody Pracodawcy oraz Administratora Systemu Informatycznego.