Załącznik Nr 1
do Zarządzenia Nr 32/05
Wójta Gminy Dobra
z dnia 18.04.2005 r.

INSTRUKCJA

dotyczącą sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dobra

I. POSTANOWIENIA OGÓLNE

§ 1

1. Niniejsza instrukcja zwana dalej „Instrukcja" określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
2. Obszarem, w którym przetwarzane są dane osobowe z użyciem sprzętu komputerowego są pokoje w Urzędzie Gminy w Dobrej o numerach 1,2,3,4,5,6,7,8,9,10,11,12,13,14, w Urzędzie Gminy w Wołczkowie o numerach 1,2,4 oraz w Dobrej przy ul. Granicznej 31 – biblioteka oraz stanowisko ds. kultury.
3. Dane osobowe mogą być przechowywane:

a/ w systemie informatycznym,

b/ w kartonach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

4. Zawarte w instrukcji zasady ochrony oraz środki i zabezpieczenia danych osobowych są zgodne z ustawą z dnia 19.08.1997 r. o ochronie danych osobowych /Dz. U. z 1997 r. Nr 133, poz. 883/ oraz z rozporządzeniem Min. Spraw Wewnętrznych w Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych /Dz. U. Nr 80, poz. 521/.

II. ZABEZPIECZENIA DANYCH OSOBOWYCH

§ 2

1. Pracownicy Urzędu zobowiązani są do dołożenia szczególnej staranności w celu ochrony danych osobowych przed dostępem osób nieuprawnionych do przetwarzania danych.
2. Pracownicy Urzędu zobowiązani są do zbierania danych lub udostępniania danych osobie, której one dotyczą w sposób uniemożliwiający wejście w ich posiadanie przez osoby trzecie, chyba, że na to otrzymały zgodę osoby, której dane dotyczą.

3. Osoby nieuprawnione do dostępu do danych osobowych mogą przebywać w pomieszczeniach, w których przechowywane są te dane wyłącznie w obecności upoważnionego pracownika Urzędu.
4. Pomieszczenia, szafy, szuflady w który przechowywane są dane osobowe powinny być pozamykane na klucz na czas nieobecności pracownika. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych powinny być wtedy zamknięte /wyłączone/.
5. Poza godzinami pracy fizyczny dostęp do budynku Urzędu i pomieszczeń, w których eksploatowane są systemy informatyczne blokują kraty i system alarmowy.

§ 3

1. W pomieszczeniach, w których przebywają osoby postronne, monitory powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane oraz powinny być automatycznie wyłączone z chwila zakończenia pracy na komputerze.
2. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczna powinny być zabezpieczone przed utratą tych danych spowodowana awarią zasilania lub zakłóceniami w sieci elektrycznej przez wyposażenie w urządzenia podtrzymujące napięci /UPS/.

III. ZARZĄDZANIE SYSTEMEM INFORMATYCZNYM

§ 4

1. System informatyczny służący do przetwarzania danych osobowych może być obsługiwany wyłącznie przez pracownika Urzędu, w zakresie nadanych im uprawnień oraz po zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych / w tym z niniejszą Instrukcja/.
   Każdy pracownik podpisuje stosowane oświadczenie.
2. W szczególnych przypadkach /np. zapobieżenie utraty zbioru danych, usunięcie awarii w pracy stanowiska komputerowego, modyfikacja oprogramowania itp./ użytkownik może dopuścić do obsługi systemu informatycznego autora programu lub przedstawiciela autora /firmy od której zostało oprogramowanie zakupione/ po uprzednim powiadomieniu administratora bezpieczeństwa informacji lub administratora danych osobowych.
3. Przeglądy i konserwacja zbiorów danych przeprowadzane są w miarę potrzeb przez uprawnione osoby pod nadzorem użytkownika programu i administratora bezpieczeństwa informacji.

. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane SA do zachowania ich w tajemnicy /zarówno w czasie zatrudnienia jak i po jego ustaniu/.

§ 5

1. Przydział identyfikatora i hasła dla pracownika – użytkownika programu w którym zawarte SA dane osobowe dokonuje administrator bezpieczeństwa informacji.
2. Administrator bezpieczeństwa informacji prowadzi ewidencję użytkowników programu, która obejmuje:
1/ imię i nazwisko użytkownika,
2/ identyfikator,
3/ data przydziału i wygaśnięcia hasła.
3. Identyfikator po wyrejestrowani użytkowania nie może być przydzielony innej osobie.
4. Zmiany hasła użytkownika SA dokonywane jednorazowo na koniec miesiąca kalendarzowego.
5. Ewidencję przechowuje się w kancelarii tajnej Urzędu.

§ 6

1. Rozpoczęcie pracy w systemie informatycznym następuje po uprzednim upewnieniu się czy nie uszkodzono sprzętu komputerowego oraz nie naruszono danych osobowych.
2. Procedura zakończenia pracy na komputerze i odłączenie źródła prądu może być poprzedzona wykonaniem kopii awaryjnych.
3. Osobami odpowiedzialnymi za tworzenie kopii awaryjnych , ich przechowywanie oraz sprawdzenie pod katem dalszej przydatności są pracownicy upoważnieni do przetwarzania danych osobowych.
4. Kopie awaryjne są ewidencjonowane i przechowywane z :
   - Referatu Finansów w pomieszczeniu kasowym,
   - Z pozostałych stanowisk pracy w kancerami tajnej.
5. Po ustaniu przydatności kopie awaryjne należy bezzwłocznie zniszczyć z fakt ten odnotować w rejestrze.

§ 7

Użytkownicy dokonują okresowo sprawdzenia obecności wirusów komputerowych, nie rzadziej niż raz w miesiącu za pomocą programu antywirusowego /w ramach posiadanych licencji/.

§ 8

1. Wydruki z danymi osobowymi wykonywane przez użytkowników przechowywane są w szafach zamykanych na zamki patentowe.
2. Wydruki, które zawierają dane osobowe i SA przeznaczone do us

2. Wydruki, które zawierają dane osobowe i SA przeznaczone do usunięcia należy zniszczyć w stopniu uniemożliwiającym ich odczytanie /cięcie w nieszczarce/.

§ 9

1. Urządzenia, dyskietki lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do:

a/ likwidacji – pozbawia się wcześniej zapisu, a w przypadki gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie /np. przeciąć, złamać/,

a/ przekazania innemu podmiotowi nie uprawnionemu do otrzymania danych osobowych – pozbawia się wcześniej zapisu tych danych,

c/ naprawy – pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby uprawnionej przez administratora danych.

Załącznik Nr 2 do Instrukcji – Oświadczenie pracownika

Administrator Danych osobowych

Załącznik Nr 3
do Zarządzenia Nr 32/05
Wójta Gminy Dobra
z dnia 18.04.2005 r.

INSTRUKCJA

POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

w:
URZĘDZIE GMINY DOBRA ul. Szczecińska 16a
URZĘDZIE GMINY DOBRA z siedzibą w WOŁCZKOWIE ul. Lipowa 51

INSTRUKCJA
postępowania w sytuacji naruszenia ochrony danych osobowych

§ 1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym.

§ 2

Instrukcja określa tryb postępowania przypadku, gdy:
1) **stwierdzono naruszenie zabezpieczenia** systemu informatycznego,
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej **mogą wskazać na naruszenie zabezpieczeń** tych danych.

§ 3

Każda osoba zatrudniona w Urzędzie Gminy, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub administratora bezpieczeństwa informacji albo inna upoważniona przez niego osobę.

§ 4

Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji lub inna upoważnioną przez niego osobę, a w przypadku ich nieobecności – bezpośrednio administratora danych osobowych.

§ 5

Administrator bezpieczeństwa informacji lub osoba upoważniona przez niego powinna w pierwszej kolejności:

1. Zapisać wszelkie **informacje związane** z danym zdarzeniem, a szczególnie: dokładny czas uzyskania informacji i naruszeniu zabezpieczenia danych

osobowych i czas samodzielnego wykrycia tego faktu.

2. Na bieżąco **wygenerować** i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie **możliwe dokumenty i raporty**, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem.

3. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osobowych niepowołanej.

§ 6

Niezwłocznie należy podjąć odpowiednie kroki w celu **powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej**, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, szczególnie przez:

a) **fizyczne odłączenie** urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieupoważnionej,
b) **wylogowanie** użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
c) **zmianę hasła** na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

§ 7

Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić **wstępną analizę stanu systemu** informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie.

§ 8

Administrator bezpieczeństwa informacji lub inna upoważniona przez niego osoba powinna sprawdzić:
a) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
b) zawartość zbioru danych osobowych,
c) sposób działania programu,
d) jakość komunikacji w sieci telekomunikacyjnej,
e) jak również wykluczyć możliwość obecności wirusów komputerowych.