Załącznik nr 2
do Zarządzenia nr .....
Starosty Ząbkowickiego
z dnia .....

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻACYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W ZĄBKOWICACH ŚL

Opracował: Administrator Bezpieczeństwa Informacji

Ząbkowice Śląskie 2009 r.

SPIS TREŚCI:

ZAŁĄCZNIKI:

Załącznik nr 1. **Wzór wniosku o nadanie uprawnień w systemie informatycznym służacym do przetwarzania danych osobowych**

Załącznik nr 2. **Wzór ewidencji użytkowników systemów i ich uprawnień**

Załącznik nr 3. **Wzór ewidencji wydania dostępu do konta administracyjnego**

Załącznik nr 4. **Wzór ewidencji wykonania kopii / odkopiowania danych systemu**

Załącznik nr 5. **Wzór dziennika awarii systemu informatycznego**

I. Podstawa prawna.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz Rozporządzenie 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 z późn. zm.)

II. Przepisy ogólne.

1. Instrukcja zarządzania systemem informatycznym Starostwa Powiatowego w Ząbkowicach Śląskich, zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy we wszystkich systemach informatycznych, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemów informatycznych Starostwa Powiatowego w Ząbkowicach Śl.
2. Niniejsza instrukcja realizuje „Politykę bezpieczeństwa systemu informatycznego" obowiązującą w Starostwie Powiatowym w Ząbkowicach Śl. z wyłączeniem systemu Pojazd i Kierowca funkcjonującego w Wydziale Komunikacji, którego warunki pracy reguluje odrębna instrukcja.

III. Definicje.

1. Ilekroć w niniejszym dokumencie jest mowa o:
   - Urzędzie – należy przez to rozumieć Starostwo Powiatowe w Ząbkowicach Śl,
   - Administratorze Danych Osobowych – należy przez to rozumieć Starostę Ząbkowickiego,
   - Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika wyznaczonego do nadzorowania przestrzegania zasad ochrony danych osobowych ustanowionych zgodnie z polityką bezpieczeństwa przetwarzania danych osobowych Urzędu,
   - Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego Urzędu oraz za stosowanie technicznych i organizacyjnych środków ochrony,
   - Użytkowniku systemu – należy przez to rozumieć osobę posiadającą uprawnienia umożliwiające dostęp do systemu informatycznego, w którym są przetwarzane dane osobowe (ewidencję użytkowników systemów i ich uprawnień prowadzi Administrator Systemów Informatycznych),

- Osobie upoważnionej - należy przez to rozumieć osobę posiadającą upoważnienie wydane przez Administratora Danych Osobowych na wniosek Administratora Bezpieczeństwa Informacji i dopuszczoną, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu (ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji),
- Sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
- Sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Do systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych. Uprawnienia umożliwiające dostęp do systemu informatycznego , w którym są przetwarzane dane osobowe przyznaje Administrator Danych Osobowych w toku następującej procedury:
   a) bezpośredni przełożony pracownika kieruje do Administratora Systemów Informatycznych wniosek o dostęp do systemu określając:
      - niezbędne dane użytkownika,
      - zbiór danych osobowych
      - zakres dostępu do systemu informatycznego,

      (wzór wniosku stanowi załącznik nr 1 do niniejszego dokumentu),
   b) Administrator Systemów Informatycznych występuje do Administratora Bezpieczeństwa Informacji o uzupełnienie we wniosku informacji dotyczących upoważnienia do przetważania danych osobowych w zbiorze, którego wniosek dotyczy a następnie przedkłada wniosek Administratorowi Danych Osobowych (Staroście) do akceptacji,
   c) po zaakceptowaniu wniosku przez Starostę Administrator Systemów Informatycznych nadaje prawa dostępu do zasobów (login i hasło umożliwiające dostęp do wszystkich systemów i aplikacji w zakresie zaakceptowanym we wniosku) oraz szkoli użytkownika w zakresie bezpiecznej obsługi urządzeń i programów.

2. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych w systemie informatycznym musi zostać zapoznany z:
   - Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.),
   - 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 z późn. zm.)
   - Polityką bezpieczeństwa przetwarzania danych osobowych systemu informatycznego,
   - Instrukcjami zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,

   oraz posiadać upoważnienie do przetwarzania danych osobowych.
3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz określenia zakresu dostępnych danych i operacji.
4. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do komputera oraz dostępu do aplikacji.
5. Hasła ustanowione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których posiada uprawnienia oraz ponosi pełną odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
7. Modyfikacja lub odebranie pracownikowi uprawnień w systemie informatycznym następuje na pisemny wniosek przełożonego pracownika i podlega analogicznej procedurze jak przy nadawaniu uprawnień.
8. Identyfikator osoby, która utraciła upoważnienie do przetważania danych osobowych lub uprawnienia dostępu do systemu informatycznego należy niezwłocznie zablokować i nie należy go nadawać innym użytkownikom.
9. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony ewidencji użytkowników i ich uprawnień w systemie informatycznym (wzór ewidencji stanowi załącznik nr 2 do niniejszego dokumentu). Ewidencja prowadzona jest na podstawie zaakceptowanych wniosków o nadanie uprawnień.

V. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane, co najmniej raz w miesiącu i jeżeli istnieje taka możliwość system powinien wymuszać zmianę hasła.
3. Identyfikator jest przypisany do użytkownika na stałe i nie należy go zmieniać ani przydzielać innemu użytkownikowi.
4. Użytkownicy 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, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.
8. Przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła - 8 znaków,
   b) zakazuje się stosować: haseł, które użytkownik stosował uprzednio w okresie minionego roku, swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.), swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp. wyrazów słownikowych, przewidywalnych sekwencji znaków z klawiatury np.: QWERTY","12345678",itp.
   c) należy stosować hasła zawierające:
      - kombinacje liter i cyfr,
      - małe i wielkie litery
      - znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala,
   d) używane hasła powinny być łatwe do zapamiętania i wykluczać konieczność ich zapisywania oraz powinny być łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,
9. W systemach, które posiadają opcję zapamiętania nazw użytkownika i jego hasła nie należy korzystać z tego ułatwienia.

10. Hasło Administratora Systemów Informatycznych o prawach administratora powinno znajdować się w zapieczętowanej kopercie w zamykanej na klucz szafie metalowej lub sejfie, do której dostęp mają:
    - Starosta,
    - Sekretarz,
    - Administrator Bezpieczeństwa Informacji.
11. Każdorazowe pobranie hasła z zapieczętowanej koperty przez osobę uprawnioną musi zostać odnotowane w ewidencji wydania dostępu do konta administracyjnego, którego wzór stanowi załącznik nr 3 do niniejszego dokumentu.
12. Po każdorazowym pobraniu hasła z zapieczętowanej koperty przez osobę uprawnioną Administrator Systemów Informatycznych ma obowiązek dokonać zmiany hasła oraz aktualne hasło ponownie umieścić w zapieczętowanej kopercie. Fakt zmiany hasła z podaniem daty należy odnotować w ewidencji.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu operacyjnego przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać czynność wylogowania z systemu (zablokowania dostępu).
3. Każdy komputer powinien mieć włączony wygaszacz ekranu ustawiony na 5 min. i aktywowaną opcję żądania podania hasła przy wznowieniu pracy.
4. Osoba udostępniająca stanowisko komputerowe innemu uprawnionemu do pracy na tym stanowisku pracownikowi zobowiązana jest wykonać operację wylogowania z systemu.
5. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów i wykonać zamknięcie systemu.
6. Niedopuszczalne jest wyłączanie komputera przed zamknięciem uruchomionego oprogramowania oraz zakończeniem pracy w sieci.
7. Czas pracy przy przetwarzaniu zbiorów danych osobowych pokrywa się z czasem pracy urzędu. Praca przy przetwarzaniu zbiorów poza tymi godzinami wymaga zgody Administratora Danych Osobowych.

VII. Procedury tworzenia zabezpieczeń.

1. Za systematyczne wykonywanie kopii bezpieczeństwa wszystkich systemów pracujących w Urzędzie odpowiada Administrator Systemów Informatycznych.
2. Kopie bezpieczeństwa wykonywane są codzienne po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
3. Kopie bezpieczeństwa wykonywane są w systemie informatycznym a następnie przenoszone na nośniki zewnętrzne (streamer, płyta CD lub płyta DVD),
   - każdy nośnik można wykorzystać do wykonania nie więcej niż 5 kopii,
   - przechowuje się, co najmniej 5 nośników zawierających dane chronologicznie wstecz.
4. Dodatkowe zabezpieczenie systemu i danych należy wykonać przed przystąpieniem do newralgicznych czynności mających wpływ na funkcjonalność oprogramowania lub zmianę struktury baz danych związanych np. z aktualizacją oprogramowania,
5. W celu sprawdzenia poprawności wykonywanych kopii należy dokonywać okresowego sprawdzenia poprawności zapisu danych (odkopiowania) oraz jego użyteczności przy odtworzeniu danych,
6. Wykonanie kopii bezpieczeństwa oraz jej weryfikację należy odnotować w ewidencji wykonanych kopii, której wzór stanowi załącznik nr 4 do niniejszego dokumentu.

VIII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

A. Elektroniczne nośniki informacji.
   1. Danych osobowych w postaci elektronicznej zapisanych na nośnikach zewnętrznych nie wolno wynosić poza siedzibę Urzędu.
   2. Komputery przenośne używane do gromadzenia lub przetwarzania danych osobowych można wynosić poza obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa jedynie po uzyskaniu pisemnej zgody Administratora Danych Osobowych.
   3. Wymienne elektroniczne nośniki informacji - za wyjątkiem kopii bezpieczeństwa - należy używać tylko w pokojach stanowiących obszar przetwarzania tych danych osobowych, określony w Polityce bezpieczeństwa.
   4. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji należy przechowywać w zamykanych szafkach biurowych.

5. Urządzenia, dyski lub inne informatyczne nośniki, 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.
6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
7. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem Administratora Systemów Informatycznych.
8. Za podjęcie czynności określonych w pkt. 5-7 odpowiada Administrator Systemów Informatycznych.

B. Kopie zapasowe.
1. Kopie bezpieczeństwa są przechowywane w sejfie w:
   - budynku przy ul. Prusa 5 w pokoju 111 i 210,
   - budynku przy ul. Sienkiewicza 11 w pokoju 107 i 309
2. Dostęp do kopii opisanych w punkcie 1 ma Administrator Systemów Informatycznych oraz upoważnieni przez Starostę pracownicy.

C. Wydruki.
1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Pomieszczenie, w którym przechowywane są wydruki zawierające dane osobowe musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do zniszczenia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

IX. Środki ochrony systemu przed złośliwym oprogramowaniem i wirusami komputerowymi.

1. Na każdym stanowisku komputerowym należy zainstalować oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do Urzędu musi być sprawdzony pod kątem występowania wirusów przez monitor antywirusowy.
3. Definicje wzorców wirusów aktualizowane są na bieżąco on-line a na stacjach roboczych pozbawionych dostępu do internetu 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 pobiera plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który otrzymał pocztę.
7. Administrator Systemu Informatycznego przeprowadza minimum raz na kwartał cykliczne kontrole antywirusowe na wszystkich komputerach .
8. Kontrola antywirusowa przeprowadzana jest również na komputerze w przypadku zgłoszenia nieprawidłowości w jego funkcjonowaniu.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

X. Procedury wykonywania przeglądów i konserwacji systemu.

A. Przeglądy i konserwacja urządzeń.
   1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach i w zakresie określonym przez producenta sprzętu.
   2. Nieprawidłowości ujawnione w trakcie działania urządzeń powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie zaistnienia nieprawidłowości w działaniu urządzeń należy niezwłocznie zawiadomić Administratora Systemów Informatycznych.

B. Przegląd i konfiguracja programów i narzędzi programowych.
   1. Konserwacja i indeksacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
   2. Administrator Systemów Informatycznych zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.
   3. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na płytę CD-R/DVD-R.

C. Rejestracja działań konserwacyjnych, awarii oraz napraw.
   1. Administrator Systemów Informatycznych prowadzi „Dziennik awarii systemów informatycznych Starostwa". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku nr 5.
   2. Wpisów do dziennika może dokonywać wyłącznie Administrator Systemów Informatycznych lub osoba go zastępująca.

XI. Połączenie do sieci Internet.

1. Połączenie lokalnej sieci komputerowej Starostwa z siecią WAN (internetem) jest realizowane wyłącznie poprzez skonfigurowaną na routerze sprzętową zaporę ogniową (firewall). Ochrona antywirusowa jest realizowana na każdym terminalu indywidualnie poprzez zainstalowane aktualne oprogramowanie antywirusowe z aktywnym monitorem antywirusowym. Za konfigurację i optymalizację pracy zapór ogniowych na routerach oraz instalację, konfiguracje i aktualizację ochrony antywirusowej na wszystkich komputerach w sieci odpowiada Administrator Systemów Informatycznych.
2. W efekcie zastosowanie zapory firewall i oprogramowania antywirusowego zapewnione jest:
   1) zabezpieczenie sieci przed atakiem z zewnątrz,
   2) filtrowanie dostępu do sieci WAN i blokowanie niektórych usług,
   3) objęcie ochroną antywirusową wszystkich danych ściąganych z internetu na stacjach lokalnych.

XII. Postanowienia końcowe.

1. W kwestiach nieuregulowanych w niniejszym dokumencie a dotyczących bezpieczeństwa danych osobowych w Starostwie Powiatowym w Ząbkowicach Śląskich decyzje na wniosek zainteresowanego wydaje Administrator Danych Osobowych (Starosta).