INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM STAROSTWA POWIATOWEGO W LIPNIE

Spis Treści

Załączniki :
Załącznik nr 1: Wykaz osób które przyjęły zapisy Instrukcji zarządzania systemem informatycznym
Załącznik nr 2: Wzór Upoważnienia
Załącznik nr 3: Rejestr użytkowników i uprawnień w systemie informatycznym
Załącznik nr 4: Ewidencja Awarii i Napraw Systemu Informatycznego
Załącznik nr 5: POCEDURA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Podstawa prawna:
_ 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)
_ ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.)

I. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:
a. **Urzędzie** - należy przez to rozumieć Urząd Starostwa Powiatowego w Lipnie,
b. **Główny Administrator Informacji** - należy przez to rozumieć Starostę Powiatu Lipnowskiego,
c. **Administratorze Bezpieczeństwa Informacji** - należy przez to rozumieć pracownika urzędu lub inną osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
d. **Administratorze Systemu Informatycznego** - należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony,
e. **użytkownika systemu** - należy przez to rozumieć osobę upoważnioną 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 lub wolontariusz,
f. **sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
g. **sieci rozległej** - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)
h. **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
i. **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów,
j. **wykazie zbiorów danych osobowych** – rozumie się przez to wykaz zarejestrowanych, oraz nie podlegających rejestracji zbiorów danych osobowych,
k. **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach Informatycznych,
l. **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

II. Procedury nadawania i zmiany uprawnień do przetwarzania danych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

_ Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.),

_ Polityką bezpieczeństwa przetwarzania danych osobowych systemu informatycznego,

_ niniejszym dokumentem.

2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **Załącznik nr 1.**

3. Przetwarzanie danych osobowych może dokonywać jedynie pracownik upoważniony przez administratora danych osobowych, którego wzór stanowi **Załącznik nr 2.**

4. Administrator bezpieczeństwa informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego.

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,

6. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym. Ustanowione hasło, administrator przekazuje użytkownikowi ustnie,

7. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

8. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu,

9. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych,

10. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

11. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: Hasło na poziomie Biosu oraz hasło dostępu do aplikacji.

12. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany na poziomie Biosu.

13. Odebranie uprawnień pracownikowi następuje na pisemny wniosek Administratora Informacji ,któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.

14 . Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.

15. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

16. Administrator bezpieczeństwa informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

17. Rejestr, którego wzór stanowi **Załącznik nr 3** powinien zawierać:

_ imię i nazwisko użytkownika systemów informatycznych,

_ rodzaj uprawnienia,

_ datę nadania uprawnienia,

_ datę odebrania uprawnienia,

_ przyczynę odebrania uprawnienia,
_ podpis administratora bezpieczeństwa informacji.
18. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

III. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.
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. Pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
9. Przy wyborze hasła obowiązują następujące zasady:
a. minimalna długość hasła - 6 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.),
_ 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,
_ hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala
_ hasła, które można zapamiętać bez zapisywania,
_ hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,
10. Zmiany hasła nie wolno zlecać innym osobom.
11. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
12.Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
a. Administrator Bezpieczeństwa Informacji
b. Starosta Powiatu lub osoba przez niego wyznaczona

IV. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wymeldowania 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 wymeldowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.
6. Przypadki stwierdzenia nieprawidłowości systemu należy zgłaszać do Administratora Systemu,który zdarzenie rejestruje w Ewidencji Awarii i Napraw Systemu Informatycznego

Załącznik nr 4

V. Procedury tworzenia zabezpieczeń

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji.
2. Kopie bezpieczeństwa wykonywane są w cyklach
2.1 tygodniowy – płyty CD-R, DVD-R
2.2 miesięczny – płyty CD-R, DVD-R
2.3 Kwartalna – płyty DVD-R
3. Płyty CD-R, DVD-R przechowuje się w sejfie urzędu
4. W przypadku wykonywania zabezpieczeń długoterminowych lub płytach CD-R, DVD-R nośniki te należy co kwartał sprawdzać pod kątem ich dalszej przydatności.

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

A. Elektroniczne nośniki informacji

1. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa - zapisane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę urzędu.
2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych urzędu.
3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.
4. 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.
5. 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.
6. 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 osoby upoważnionej.

B. **Kopie zapasowe**

1. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w sejfie urzędu.
2. Dostęp do ww. sejfu mają tylko upoważnieni 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 robocze musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

VII. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

1. Na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do urzędu musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.
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 odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika dyskietki.

VIII. W razie stwierdzenia naruszenia ochrony danych osobowych postępujemy zgodnie z procedurą Załącznik nr 5

IX. Zasady udostępniania danych oraz rejestracji zbiorów danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie na wniosek do Administratora Danych
2. Udostępnienie zbiorów danych może nastąpić po wyrażeniu zgody przez Administratora Danych oraz Administratora Bezpieczeństwa Informacji. Zgoda nie jest wymagana, jeśli udostępnienie danych wynika z zakresu zadań tej jednostki organizacyjnej

Starostwa, w dyspozycji której znajdują się te dane,
3. Administrator Bezpieczeństwa Informacji może odmówić udostępnienia danych jeżeli może to naruszyć bezpieczeństwo i ochronę danych zgromadzony w Systemie Informatycznym Starostwa.

X. Połączenie do sieci Internet

1. Połączenie lokalnej sieci komputerowej urzędu z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych oraz kompleksowego oprogramowania antywirusowego.
2. Do zabezpieczenia sieci należy stosować
a. Firewall,
b. Systemy wykrywania włamań IDS
c. Rejestracja wszelkich zdarzeń w dziennikach systemowych
d. Systemy antywirusowe i antyszpiegowskie.