KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Załącznik nr.2 do Zarządzania nr 54/2015
Burmistrza Miasta i Gminy Chmielnik
Z dnia 30 marca.2015 roku

Instrukcja Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych

Urzędu Miasta i Gminy w Chmielniku

Projekt „e-Urząd – satysfakcja, komfort i wygoda dla Mieszkańców" współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

Urząd Miasta i Gminy

Chmielnik

• • •

• • •

26-020 Chmielnik

Plac Kościuszki 7

Powiat Kielecki

Województwo
Świętokrzyskie

• • •

www.chmielnik.com

umig@chmielnik.com

Wstęp

Celem wydania dokumentu jest realizacja zapisów „Polityki Bezpieczeństwa" przetwarzania danych osobowych obowiązującej w Urzędzie Miasta i Gminy w Chmielniku oraz postanowień §5 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.

Spis treści

1. Definicje

Ilekroć w niniejszej Instrukcji Zarządzania Systemem Informatycznym mowa o:

1) **komórce organizacyjnej** – rozumie się przez to odpowiednio wydziały i komórki organizacyjne, o których mowa w §17 Regulaminu Organizacyjnego Urzędu Miasta i Gminy w Chmielniku stanowiącego załącznik do Zarządzenia 47/2015 Burmistrza Miasta i Gminy w Chmielniku z dnia 11 marca 2015 r.

2) **Kierowniku komórki organizacyjnej** – rozumie się przez to kierownika wydziału, referatu, biura, koordynatora i samodzielne stanowiska pracy;

3) **Administratorze Danych Osobowych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. Administratorem Danych Osobowych jest Burmistrz Miasta i Gminy Chmielnik;

4) **Administratorze Bezpieczeństwa Informacji** – rozumie się przez to pracownika Urzędu Miasta i Gminy wyznaczonego przez Administratora Danych Osobowych, nadzorującego przestrzeganie zasad, o których mowa w art. 36 ust. 1 u.o.d.o.;

5) **Administratorze Systemów Informatycznych** – rozumie się przez to pracownika Urzędu Miasta i Gminy, odpowiedzialnego za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

6) **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik Urzędu Miasta i Gminy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.

7) **Osobie nieupoważnionej** – rozumie się przez to osobę nieposiadającą upoważnienia do przetwarzania danych osobowych;

8) **Osobie nieuprawnionej** – rozumie się przez to osobę nieposiadającą uprawnień nadanych w systemie informatycznym Urzędu Miasta i Gminy;

9) **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na

numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;

10) **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

11) **Przetwarzaniu danych osobowych** – 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;

12) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

13) **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

14) **Bezpieczeństwie informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania informacji by w każdych okolicznościach dostęp do nich był zgodny z założeniami;

15) **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

16) **Zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie;

17) **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe za wyjątkiem:

   a) osoby, której dane dotyczą,

   b) osoby upoważnionej do przetwarzania danych osobowych,

c) przedstawiciela, o którym mowa w art. 31a u.o.d.o.,

d) podmiotu, o którym mowa w art. 31 u.o.d.o.,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

18) **Państwie trzecim** – rozumie się przez to państwo należące do Europejskiego Obszaru Gospodarczego;

19) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi uprawnionemu do pracy w systemie informatycznym;

20) **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w wyznaczonych przez Administratora Danych Osobowych obszarach systemu informatycznego Urzędu Miasta i Gminy;

21) **Teletransmisji danych** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnych;

22) **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

23) **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

24) **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub podmiotowi;

25) **Użytkowniku systemu informatycznego** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych, której nadano unikalny identyfikator i hasło

26) **Uwierzytelnieniu** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym Urzędu Miasta i Gminy;

27) **Sieci komputerowej** – rozumie się przez to grupę komputerów lub innych urządzeń połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów;

28) **Sieci lokalnej** – rozumie się przez to sieć przeznaczoną do łączenia ze sobą stanowisk komputerowych znajdujących się w Urzędzie Miasta i Gminy;

29) **Sieć publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 ust. 22 ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. nr 73, poz. 852 z późn. zm.);

30) **Punkcie dystrybucyjnym** – rozumie się przez to miejsce, w którym zlokalizowana jest infrastruktura teleinformatyczna oraz urządzenia umożliwiające dystrybucję połączeń sieciowych w systemie informatycznym Urzędu Miasta i Gminy;

31) **Stacji roboczej** – rozumie się przez to komputer użytkownika systemu informatycznego podłączony do sieci lokalnej Urzędu Miasta i Gminy;

32) **Incydent** – rozumie się przez to naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;

33) **Zagrożenie** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;

34) **Działa korygujące** – rozumie się przez to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;

35) **Działania zapobiegawcze** – rozumie się przez to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.

1. Wprowadzenie

Instrukcja została opracowana zgodnie z wymogami §5 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).

Niniejsza instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych oraz w systemach informatycznych Urzędu Miasta i Gminy w Chmielniku. Instrukcja powstała w celu realizacji zapisów „Polityki Bezpieczeństwa" przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Chmielniku i jest z nią komplementarna.

2. Zakres stosowania Instrukcji Zarządzania Systemem Informatycznym

Procedury i zasady określone w niniejszym dokumencie powinny być znane i stosowane przez wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym Urzędu Miasta i Gminy w Chmielniku, bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy.

3. Podstawy prawne

Instrukcja Zarządzania Systemem Informatycznym odnosi się do sposobu przetwarzania danych osobowych oraz środków ich ochrony wraz z określeniem warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do ich przetwarzania, określone w:

1) ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, ze zm.)

2) rozporządzeniu 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. z 2004r., Nr 100, poz. 1024).

4. Zasady bezpiecznej eksploatacji systemu informatycznego

1) Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się **„poziom wysoki"** bezpieczeństwa w rozumieniu § 6 rozporządzenia.

2) W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, dostęp do systemu informatycznego powinien być możliwy wyłącznie po podaniu identyfikatora odrębnego dla każdego użytkownika systemu i poufnego hasła lub innego elementu uwierzytelniającego.

3) Należy zapewnić poufność, integralność i rozliczalność danych osobowych przetwarzanych w systemie informatycznym Urzędu Miasta i Gminy.

4) Należy zapewnić, aby użytkownicy systemu informatycznego służącego do przetwarzania danych osobowych nie posiadali wyższych poziomów uprawnień w tym systemie niż wymagane jest to do wykonywania powierzonych obowiązków.

5) Prawidłowy poziom zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych zostaje zapewniony poprzez przestrzeganie następujących zasad:

a) uniemożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemu informatycznego,

b) niepodejmowanie przez użytkowników systemu prób wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie, a także poprzez instalowanie nowego lub aktualizowanie już zainstalowanego oprogramowania,

c) korzystanie z systemu informatycznego dla celów innych niż związane z wykonywaniem obowiązków służbowych jest zabronione.

6) Dostęp do poszczególnych usług systemu informatycznego powinien być chroniony kontrolą dostępu.

7) Przesyłanie danych osobowych drogą teletransmisji odbywa się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.

8) Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych.

9) Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane, a logi połączeń archiwizowane w trybie ciągłym.

10) Użytkownicy systemu powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym oraz w związku ze zmiana przepisów o ochronie danych osobowych lub zmiana wewnętrznych regulacji.

5. Zasady przetwarzania danych w zbiorach doraźnych

1) Dostęp do danych osobowych powinien odbywać się poprzez dedykowane aplikacje, działające w architekturze klient-serwer, lub przynajmniej, przechowujące dane na serwerach plików, nie zaś na indywidualnych stanowiskach komputerowych pracowników.

2) Wyłącznie w sytuacjach wyjątkowych dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdująca się w określonym systemie informatycznym. Rejestry zawierające dane osobowe wykonywane w plikach (MS Word, MS Excel) mają tylko charakter tymczasowy i pomocniczy dla dokumentacji papierowej.

3) Przetwarzanie danych na stacji lokalnej lub w innym formacie, np. dane do raportu w postaci pliku arkusza kalkulacyjnego, możliwe jest pod warunkiem, iż zapisane dane będą należycie chronione, tj.

a) uniemożliwi się dostęp do danych osobom nieuprawnionym,

b) uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu,

c) zabezpieczy się bezpośredni dostęp do danych hasłem.

4) Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych.

6. Zasady postępowania z komputerami przenośnymi

1) Użytkownik systemu informatycznego, używający komputer przenośny zawierający dane osobowe, zobowiązany jest zachować szczególna ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.

2) Użytkownik systemu informatycznego używający komputer przenośny zawierający dane osobowe w szczególności powinien:

a)stosować ochronę kryptograficzna;

b) zabezpieczyć dostęp do komputera przenośnego na poziomie systemu operacyjnego - identyfikator i hasło;

c) nie zezwalać na używanie komputera przenośnego osobom nieupoważnionym;

d) zachować szczególna ostrożność przy podłączaniu do sieci publicznych.

3) Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

7. Procedura nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym

Zasady regulujące nadawanie uprawnień do przetwarzania danych oraz rejestrowania uprawnień w systemie informatycznym określono w procedurze **PRO_1 - „Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym."**

Procedura obowiązuje wszystkie osoby zaangażowane w proces nadawania uprawnień w systemie informatycznym, a w szczególności kierowników komórek organizacyjnych lub bezpośrednich przełożonych użytkowników systemu informatycznego, Administratora Systemu Informatycznego, a także Administratora Bezpieczeństwa Informacji.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

8. Stosowane metody i środki uwierzytelniania oraz procedury związanych z ich zarządzaniem i użytkowaniem

Zasady dotyczące stosowanych metod i środków uwierzytelniania w systemie informatycznym Urzędu Gminy określono w procedurach:

a) **PRO_2 - „Stosowane metody i środki uwierzytelniania. Ogólne zasady";**
b) **PRO_3 - „Stosowane metody i środki uwierzytelniania. Hasła administracyjne".**

Procedury obowiązują wszystkie osoby mające uprawnienia do przetwarzania danych osobowych w systemie informatycznym, a także Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszych procedur.

9. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

Zasady dotyczące rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym określono w procedurze **PRO_4 - „Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym".**

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym Urzędu Miasta i Gminy.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

10. Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Zasady dotyczące tworzenia kopii zapasowych zawierających dane osobowe, a także programów i narzędzi wykorzystywanych do przetwarzania danych określono w procedurze **PRO_5 - „Tworzenie kopii zapasowych zbiorów danych osobowych".**

Procedura obowiązuje Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

11. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Zasady dotyczące sposobu, miejsca i okresu przechowywania zarówno elektronicznych nośników informacji jak i kopii zapasowych zawierających dane osobowe określono w procedurze **PRO_6 - „Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych".**

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym przy użyciu elektronicznych nośników informacji, a także Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

12. Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania

Zasady dotyczące stosowania profilaktyki antywirusowej określono w procedurze **PRO_7 - „Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania".**

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym, a także Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

13. Odnotowywanie w systemie informatycznym informacji o udostępnianiu danych

Zasady dotyczące odnotowywania informacji w systemie informatycznych, o których mowa w §7 ust. 1 pkt 4 rozp. MSWIA określono w procedurze **PRO_8 - „Odnotowanie w systemie informacji i udostępnianiu danych".**

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

14. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Zasady dotyczące wykonywania przeglądów i konserwacji systemów informatycznych oraz nośników informacji służących do przetwarzania danych określono w procedurze **PRO_9 - „Wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych".**

Procedura obowiązuje Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

15. Procedury

PRO_1 - „Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym."

PRO_2 - „Stosowane metody i środki uwierzytelniania. Ogólne zasady";

PRO_3 - „Stosowane metody i środki uwierzytelniania. Hasła administracyjne".

PRO_4 - „Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym".

PRO_5 - „Tworzenie kopii zapasowych zbiorów danych osobowych".

PRO_6 - „Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych".

PRO_7 - „Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania".

PRO_8 – „Realizacja wymogów, o których mowa w § 7 ust.1 pkt 4 rozp. MSWIA."

PRO_9 - „Wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych".