Załącznik nr 2 do Zarządzenia Nr 93 /2013
Wojewody Świętokrzyskiego
z dnia 2 października 2013 roku

INSTRUKCJA

ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

……..….

SŁUŻĄCYM DO PRZETWARZANIA DANYCH

OSOBOWYCH

KIELCE 2013

I. Wstęp

Instrukcja określa sposób zarządzania systemem informatycznym …….., w którym przetwarza się dane osobowe w …….. Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach. Procedury w zakresie zasad bezpiecznej eksploatacji systemu uwzględniają postanowienia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz 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).

II. Definicje pojęć zastosowanych w instrukcji

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Administrator danych osobowych - osoba decydująca o organizacji, zasadach eksploatacji i udostępnianiu danych osobowych.

Administrator systemu - pracownik Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach, odpowiedzialny za realizację zadań związanych z eksploatacją systemu informatycznego ……...……. Przetwarzającego dane osobowe, ze szczególnym uwzględnieniem dystrybucji haseł dostępu i uprawnianiem technicznym osób do dostępu do systemu na podstawie pisemnej decyzji administratora danych.

Administrator sieci komputerowej - pracownik Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach, odpowiedzialny za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.

Administrator bezpieczeństwa informacji - pracownik Świętokrzyskiego Urzędu Wojewódzkiego wyznaczony przez administratora danych osobowych odpowiedzialny za zabezpieczenie systemu informatycznego tzn. analizę zagrożeń, wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów systemu teleinformatycznego oraz ochrony przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, pozyskaniem danych osobowych lub ich utratą.

III. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Osobą odpowiedzialną za nadawanie uprawnień dostępu do systemu informatycznego …….. jest administrator systemu informatycznego.
2. Dostęp do systemu informatycznego mogą uzyskać tylko pracownicy posiadający upoważnienia zgodnie z załącznikiem Nr 3 niniejszej instrukcji.
3. W wyjątkowych przypadkach, np.: nieobecności administratora systemu, powyższe czynności może wykonywać osoba wyznaczona przez administratora danych osobowych oraz administrator sieci komputerowej ŚUW.
4. Jeżeli system informatyczny ……..……. wymaga zdefiniowania identyfikatora i hasła użytkownika o uprawnieniach administratora systemu, to tym identyfikatorem i hasłem powinien się posługiwać wyłącznie administrator systemu informatycznego z wyjątkiem sytuacji opisanej w punkcie 3.

IV. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W przypadku, gdy system informatyczny ……, który zawiera dane osobowe ma postać plików przetwarzanych na pojedynczym komputerze w programach pakietu biurowego typu „Office” (pliki edytora tekstu lub arkusze kalkulacyjne), wtedy użytkownik danych osobowych zobowiązany jest zabezpieczyć każdy plik hasłem zgodnym z wymaganiami pkt 5,6,7.
2. W przypadku, gdy system informatyczny …….. który przetwarza dane osobowe nie ma postaci opisanej w pkt 1, wtedy dla każdego użytkownika systemu informatycznego administrator systemu ustala odrębny identyfikator i hasło.

3. Dostęp do danych osobowych przetwarzanych w systemie może odbywać się wyłącznie po podaniu identyfikatora i właściwego hasła.
4. Identyfikator, o którym mowa wyżej wpisuje się do ewidencji określonej w art. 39 ust. 1 ustawy o ochronie danych osobowych wraz z imieniem i nazwiskiem użytkownika oraz rejestruje w systemie informatycznym
5. Hasło użytkownika należy zmieniać nie rzadziej jak jeden raz na miesiąc.
6. Hasło użytkownika powinno składać się, co najmniej z 8 znaków, jeżeli w systemie nie są przetwarzane dane, o których mowa w art. 27 ustawy lub 8 znaków, jeżeli takie dane są przetwarzane (pkt VII załącznika). Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej.
7. Hasła użytkownika nie wolno nigdzie zapisywać, ani na papierze, ani w postaci elektronicznej - należy je zapamiętać.
8. Jeżeli system informatyczny ……..……. wymaga zdefiniowania identyfikatora i hasła użytkownika o uprawnieniach administratora systemu, to należy to hasło i identyfikator przechowywać w zaklejonej kopercie w metalowym sejfie zamykanym na klucz w pomieszczeniu ……
9. Identyfikatory, które utraciły ważność należy wyrejestrować, a ich hasła unieważnić.

V. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Przed rozpoczęciem pracy użytkownik powinien sprawdzić, czy stan sprzętu komputerowego nie wskazuje na próbę uruchomienia komputera przez osobę niepowołaną.
2. Użytkownicy uzyskują bezpośredni dostęp do danych w systemie po podaniu identyfikatora i właściwego hasła.
3. W przypadku pozostawienia stacji roboczej bez nadzoru użytkownik powinien bezwarunkowo wylogować się z systemu informatycznego …….. służącego do przetwarzania danych osobowych.
4. W przypadku pozostawienia stacji roboczej nieużytkowanej (powyżej 10 min) należy stosować wygaszacz ekranu na hasło.

5. W wypadku, gdy dostęp do pomieszczenia mogą mieć osoby postronne opuszczając pomieszczenie należy bezwzględnie wylogowywać się z systemu informatycznego ……....

6. Kończąc pracę użytkownik powinien:

   1) zamknąć program oraz wyjść z systemu i wyłączyć komputer wraz z drukarką,

   2) sprawdzić, czy pozostawione stanowisko nie stwarza jakichkolwiek zagrożeń i czy są prawidłowo zabezpieczone przed uruchomieniem ich przez osoby postronne.

7. Wszystkie zauważone usterki i mankamenty na stanowisku użytkownik winien natychmiast zgłosić Administratorowi Systemu Informatycznego, odpowiednim służbom konserwacyjnym oraz Administratorowi Bezpieczeństwa Informacji.

VI. Procedury tworzenia kopii zapasowych zbiorów danych oraz programy i narzędzia programowe służące do ich przetwarzania

1. Na potrzeby zachowania ciągłości działania systemu informatycznego ……. i utrzymania integralności danych wykonuje się kopie awaryjne zbiorów danych. Zadanie to realizowane jest raz w tygodniu.
2. Kopie awaryjne wykonuje administrator sieci komputerowej ŚUW.
3. W wyjątkowych przypadkach, np.: nieobecności administratora systemu, kopie awaryjne może wykonywać osoba wyznaczona przez administratora danych osobowych oraz administrator sieci komputerowej ŚUW.
4. Opis nośników z kopiami awaryjnymi powinien zawierać następujące dane:
   - System <nazwa systemu>
   - Data <rrrr. mm. dd>
   - Opis <opis zawartości nośnika>
   - Podpis < podpis osoby wykonującej kopię>

VII. Sposób, miejsce i okres przechowywania:

a) elektronicznych nośników informacji zawierających dane osobowe,

1. Elektroniczne nośniki informacji zawierające dane osobowe związane z systemem informatycznym …….. powinny być zabezpieczone przed nieumyślnym skasowaniem oraz przechowywane w metalowym sejfie zamykanym na klucz w pomieszczeniu ……..

b) kopii zapasowych, o których mowa w § 5 pkt 4 rozporządzenia.

1. Kopie zapasowe, wykonane w danym tygodniu przechowywane są przez okres 4 tygodni oraz zabezpieczone są przed nieumyślnym skasowaniem i przechowywane w metalowym sejfie zamykanym na klucz w pomieszczeniu …….
2. Kopie zapasowe sprawdzane są okresowo pod kątem ich dalszej przydatności przez administratora systemu nie rzadziej niż raz na miesiąc.
3. Po stwierdzeniu nieprzydatności kopii zapasowych zbiorów nośnik zostaje pozbawiony danych lub zniszczony w sposób uniemożliwiający dalszy odczyt informacji.
4. Wszelkie wydruki technologiczne po ich wykorzystaniu podlegają natychmiastowemu zniszczeniu lub rejestracji.

VIII. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia)

1. Systemy ochrony zastosowane na komputerach przetwarzających dane osobowe nie powinny dopuszczać możliwości zainfekowania wirusami i programami, których celem jest uzyskanie nieuprawnionego dostępu do tych komputerów.
2. Na każdej stacji roboczej wykorzystywanej do przetwarzania danych osobowych w systemie informatycznym …… wymagane jest zainstalowanie indywidualnego programu antywirusowego wraz z aktywnym modułem do bieżącego monitoringu wirusów oraz zabezpieczenia przed działaniem programów, których celem jest uzyskanie nieuprawnionego dostępu do tych stacji roboczych.
3. W programach użytkowych należy, jeśli to możliwe, uaktywnić ich wewnętrzny system ochrony przed wirusami MAKRO (programy MS Word, MS Excel itp.)
4. Zabrania się umieszczania w urządzenia odczytujących dane (stacje dyskietek,

czytniki CD-ROM, DVD, ZIP, MO itp.) nośników rozprowadzanych z różnego rodzaju czasopismami, materiałami reklamowymi itp.

5. Zabrania się wykorzystywania jakichkolwiek urządzeń służących do transmisji i magazynowania danych niestanowiących standardowego wyposażenia stanowiska komputerowego - w szczególności komputerów przenośnych - bez zgody administratora sieci komputerowej.
6. Należy używać wyłącznie nośników danych, które są oznaczone zgodnie z instrukcją.
7. Każdą dyskietkę lub inny nośnik danych - chociażby był oznaczony zgodnie z instrukcją - używany do przenoszenia danych pomiędzy stanowiskami komputerowymi, należy sprawdzić programem antywirusowym przed odczytaniem danych.
8. Jeśli program antywirusowy stwierdził istnienie wirusa na nośniku danych, taki nośnik należy natychmiast wyjąć z czytnika (stacji dyskietek, czytnika CD-ROM itp.) wyraźnie oznaczyć i przekazać nośnik administratorowi sieci komputerowej. Następnie należy przeprowadzić kontrolę antywirusową całego systemu.
9. Jeśli program antywirusowy stwierdził obecność wirusa w systemie, jeśli to możliwe, zezwolić programowi antywirusowemu na usunięcie wirusów. Jeśli program antywirusowy nie będzie mógł usunąć wirusów nie niszcząc części lub całości zbioru zainfekowanego wirusem, należy przerwać działanie programu antywirusowego i natychmiast zgłosić ten fakt administratorowi sieci komputerowej oraz administratorowi systemu informatycznego.

IX. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.
4. Pracownik, który udostępnia dane osobowe ma obowiązek prowadzenia rejestrów udostępnionych danych osobowych, który musi zawierać, co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję, dla której dane udostępniono.

5. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych osobowych. Zakres informacji powinien obejmować, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

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

1. Przegląd systemu oraz baz danych odbywa się na wniosek administratora danych osobowych i jest realizowany przez pracowników Oddziału ds. Informatyki lub przez inne upoważnione osoby.
2. Niesprawne nośniki danych, na których przechowywane są dane osobowe powinny być niszczone trwale, aby nie był możliwy odczyt z nich jakikolwiek danych.
3. W przypadku zbywania komputerów lub nośników wykorzystywanych dotychczas w systemie informatycznym …….. zawarte na przekazywanych nośnikach dane winny być nieodwracalnie wykasowywane.
4. Jeśli naprawa nośnika danych możliwa jest tylko w specjalistycznym serwisie, a istnieje konieczność odzyskania danych z tego nośnika/urządzenia, to należy podpisać osobną umowę lub uzyskać pisemną gwarancję od firmy świadczącej serwis o niewykorzystywaniu przez nią i nie przekazywaniu innym podmiotom danych należących do ŚUW.

XI. Postanowienia końcowe

Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych powinien zostać zapoznany z niniejszą instrukcją i potwierdzić podpisem przyjęcie do wiadomości obowiązek jej stosowania. Wykaz potwierdzeń prowadzi Administrator Bezpieczeństwa Informacji (załącznik nr 1).

Instrukcja wchodzi w życie z dniem jej zatwierdzenia przez Dyrektora Wydziału……. , który wykonuje kompetencje administratora danych osobowych systemu informatycznego …… służącego do przetwarzania danych osobowych.

Wzory dokumentów

Załącznik Nr 1 do instrukcji

Wykaz osób, które zostały zapoznane z instrukcją zarządzania systemem informatycznym ……. służącym do przetwarzania danych osobowych.			
Przyjąłem/łam/ do wiążącej wiadomości i stosowania postanowienia instrukcji zarządzania informatycznym systemem przetwarzania danych osobowych			
Lp.	Imię i nazwisko	Podpis	Data
1			
2			
3			
4			
5			
6			
7			

Załącznik Nr 2 do instrukcji

Wniosek o dopuszczenie osoby do pracy na stanowisku przewidzianym do przetwarzania danych osobowych

Dane osoby wnioskowanej:

Imię i nazwisko .....

Stanowisko służbowe .....

Jednostka organizacyjna .....

Lokalizacja stanowiska .....

(adres, nr pokoju, telefon, fax)

Przeznaczenie stanowiska (zakres uprawnień i odpowiedzialności):

…….

Osoba wnioskowana:

• odbyła przeszkolenie w zakresie ochrony informacji niejawnych wymagane przepisami ustawy z dnia 22stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95) i posiada zaświadczenie nr.....

• została zapoznana z obowiązującymi przepisami w zakresie ochrony danych osobowych dnia.....

• została przeszkolona do pracy na określonym stanowisku i z określonymi aplikacjami.

(podpis osoby wnioskowanej)

(stanowisko i podpis administratora bezpieczeństwa informacji)

(miejscowość, data, podpis)

(podpis administratora danych osobowych)

Nazwa stanowiska w systemie, identyfikator ID, adres IP stanowiska:

Przydzielone uprawnienia:

Administrator systemu
Brak przeciwwskazań do dopuszczenia do dostępu lub do pracy w systemie

(miejscowość, data, podpis)

Załącznik Nr 3 do instrukcji

UPOWAŻNIENIE NR...../(*Rok wydania*)

Na podstawie art. 37 ustawy o ochronie danych osobowych upoważniam

Imię i nazwisko:

Jednostka organizacyjna:

do pracy na stanowisku

(nazwa stanowiska)

przewidzianym do dostępu lub do pracy w systemie

……

do odwołania.

Kielce, dnia .....

(podpis administratora danych osobowych)