# *INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM*

## Spis treści

# 1. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych, przez administratora danych – w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

# 2. Nadawanie i rejestrowanie uprawnień.

a. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez administratora systemu na polecenie administratora danych.

b. Administrator systemu jest obowiązany upoważnić co najmniej jednego pracownika do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności dłuższej niż 14 dni.

c. Rejestracja, o której mowa w pkt b, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do ewidencji osób upoważnionych do przetwarzania danych prowadzonej wg załącznika nr 5 do Polityki bezpieczeństwa.

# 3. Odebranie uprawnień.

a. Odebranie uprawnień użytkownika systemu informatycznego wykonuje administrator systemu na polecenie administratora danych.

b. Odebranie uprawnień, o którym mowa w pkt. a, może mieć charakter czasowy lub trwały. W przypadku trwałego odebrania uprawnień administrator danych odnotowuje ten fakt w ewidencji osób upoważnionych do przetwarzania danych osobowych wg załącznika nr 5 do Polityki bezpieczeństwa.

c. Odebranie uprawnień następuje poprzez odebranie komputera i zablokowanie konta użytkownika,

d. Czasowe odebranie uprawnień użytkownika z systemu informatycznego następuje w razie:

   i. nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,

   ii. zawieszenia w pełnieniu obowiązków służbowych.

e. Przyczyną czasowego odebrania uprawnień użytkownika systemu informatycznego może być:

   i. wypowiedzenie umowy o pracę,

   ii. wszczęcie postępowania dyscyplinarnego.

f. Przyczyną trwałego odebrania uprawnień użytkownika systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

# 4. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

# I. Identyfikator

a. Administrator systemu ma pełną dowolność w doborze nazw użytkowników systemu operacyjnego komputera przydzielonego pracownikowi. Nie stosuje się żadnych schematów w tym zakresie, ogólną zasadą jest, że w systemie nie mogą istnieć dwa konta użytkownika o tej samej nazwie.

b. Konta użytkowników pozwalające na korzystanie z dysku sieciowego są tworzone na wniosek administratora danych przez wykonawcę outsourcingu usług informatycznych.

c. W przypadku kont tworzonych w systemach powierzonych za tworzenie kont użytkowników odpowiada administrator systemu jednostki powierzającej dane w sposób określony w umowie powierzenia.

## II. Hasło użytkownika

a. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

b. Każdy użytkownik jest zobowiązany do zmiany haseł do wszystkich udostępnionych mu kont przynajmniej raz na 30 dni.

c. Administrator danych i administrator systemu może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

d. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

e. Zabrania się pracownikom zapisywania haseł dostępu lub przechowywania ich w formie, która nie zapewnia poufności hasła.

f. W przypadku podejrzenia kompromitacji hasła użytkownik jest zobowiązany do natychmiastowej jego zmiany.

g. Dopuszcza się inne zasady tworzenia haseł użytkowników, które mogą wynikać z umów powierzenia jednak tylko wtedy gdy dają one dalej idącą ochronę.

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

A. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie i komputera, a następnie wprowadzeniu indywidualnego identyfikatora i znanego tylko użytkownikowi hasła.

B. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w obecności użytkownika albo osoby upoważnionej do przetwarzania danych.

C. Ustawienie monitorów powinno uniemożliwiać osobom nieupoważnionym pogląd wyświetlanych treści.

D. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.

E. Jednostkowe dane chronione (np. osobowe) mogą być kopiowane na nośniki po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.

F. Przesyłanie danych osobowych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.

G. Przetwarzając dane należy odpowiednio często wykonywać kopie robocze danych, tak by zapobiec ich utracie i umieszczać je w odpowiednich zasobach dysku sieciowego.

H. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu przetwarzanych informacji w odpowiednie obszary dysku sieciowego, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w listwie przeciwprzepięciowej.

I. Przed opuszczeniem pokoju należy:

a. zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,

b. schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,

c. umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,

d. zamknąć okna.

J. Komputery powierzone pracownikom wynoszone poza Biuro, powinny być chronione przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.

K. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.

L. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem administratora systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zwrócić się do administratora systemu.

M. Komputery wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację system wymusza automatycznie.

N. Komputery posiadają szyfrowane dyski twarde, uniemożliwiające dostęp do danych osobom postronnym.

## 6. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

A. Kopie zapasowe wykonywane są zgodnie z zapisami umowy outsourcingu usług informatycznych.

B. Dostęp do kopii bezpieczeństwa mają tylko: administrator danych, administrator systemu i pracownik usługodawcy usług informatycznych odpowiedzialny za wykonywanie kopii zapasowych zasobów dysku sieciowego.

C. Formę kopii i tryb ich wykonywania określa umowa outsourcingu usług informatycznych.

## 7. Częstotliwość wykonywania kopii

Tworzy się następujące kopie zapasowe:

A. miesięczne – na koniec miesiąca. Zakres wykonywania kopii miesięcznych określa umowa outsourcingu usług informatycznych.

## 8. Testowanie kopii

W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy je okresowo testować. Zasady testowania kopii określa umowa outsourcingu usług informatycznych Test kopii polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych. W przypadku nieudanej próby odtworzenia danych usługodawca usług informatycznych powinien poinformować administratora danych oraz wykonać jak najszybciej test ostatniej kopii zapasowej a w przypadku nieudanej próby odczytu danych wykonać nową kopie bezpieczeństwa.

## 9. Likwidacja nośników zawierających kopie

A. Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się komisyjnie. Z czynności likwidacji nośników powinien powstać protokół dla administratora systemu.

B. Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.

C. Nośniki wielorazowego użytku, które nie nadają się do ponownego użycia należy zniszczyć fizycznie.

## 10. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

A. Zbiory danych przechowywane są na dysku sieciowym. Wszelkie dane przetwarzane na poszczególnych stacjach roboczych są niezwłocznie, a najpóźniej przed zakończeniem pracy w systemie, umieszczane na dysku sieciowym w miejscach przydzielonych każdemu użytkownikowi przez administratora systemu.

B. Zakazuje się przetwarzania danych osobowych na jakichkolwiek zewnętrznych nośnikach bez zgody administratora danych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.

C. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia nośnika programem antywirusowym.

D. Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

E. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

## 11. Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

A. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na stacjach roboczych.

B. Oprogramowanie, o którym mowa w pkt 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu operacyjnego stacji roboczej.

C. Aktualizacja oprogramowania antywirusowego wykonuje się automatycznie. Do obowiązków administratora systemu należy nadzór nad poprawnością aktualizacji oprogramowania antywirusowego, określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie oraz nadzór nad realizacją i aktualnością umowy licencyjnej.

D. Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

E. Dostęp do Internetu możliwy jest na wszystkich stacjach roboczych, specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem Firewall.

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

A. Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.

B. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale administratora systemu nie rzadziej niż raz na miesiąc.

C. Kontrole i testy przeprowadzane przez administratora systemu powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

## 13. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

A. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym administratora danych przeprowadzane są zgodnie z zapisami umowy outsourcingu usług informatycznych oraz umów gwarancyjnych i serwisowych.

B. Naprawy i zmiany w systemie informatycznym administratora danych prowadzone są pod nadzorem administratora systemu w siedzibie administratora danych.

C. Przekazanie sprzętu do naprawy poza siedzibą administratora danych jest możliwe po uprzednim, nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

D. Jeśli nośnik danych (np.: dysk) zostanie uszkodzony i nie można odczytać jego zawartości ani usunąć danych, należy zniszczyć mechanicznie.

## 14. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

A. Użytkownik zobowiązany jest zawiadomić administratora danych lub uprzednio wskazanego przez niego pracownika o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

   a. naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),

   b. częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,

   c. braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,

   d. wykryciu wirusa komputerowego,

   e. zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,

   f. znacznym spowolnieniu działania systemu informatycznego,

   g. podejrzeniu kradzieży sprzętu komputerowego, nośników lub dokumentów zawierających dane osobowe,

   h. zmianie położenia sprzętu komputerowego,

   i. zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

B. Do czasu przybycia na miejsce administratora danych lub wskazanego przez niego pracownika należy:

   a. o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, z uwzględnieniem możliwości ustalenia przyczyn lub sprawców,

   b. rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

   c. zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

   d. zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,

   e. przygotować opis incydentu,

   f. nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia administratora danych lub osoby przez niego wskazanej.

C. Administrator danych po otrzymaniu zawiadomienia, o którym mowa w pkt 1, powinien niezwłocznie:

   a. przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,

   b. podjąć działania chroniące system przed ponownym wystąpieniem naruszenia,

D. Administrator systemu może zarządzić, w razie umotywowanej potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

E. W razie odtwarzania danych z kopii zapasowych administrator systemu obowiązany jest upewnić się, czy odtwarzane dane zostały zapisane przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).

F. W przypadku gdy incydent nosi znamiona czynu zabronionego administrator danych natychmiast informuje odpowiednie organy i postępuje wg ich wskazówek

G. Wszyscy pracownicy zobowiązani są do informowania administratora danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez innych użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

H. Administrator danych uwzględnia dokumentację z zaistniałych incydentów podczas wykonywania corocznej analizy ryzyka.

# 15. Postanowienia końcowe

A. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

B. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.

C. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.