Instrukcja zarządzania systemem informatycznym do przetwarzania danych osobowych

Uniwersytet Przyrodniczy w Lublinie

Spis treści

I. 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.

II. Definicje

1. Administratorze bezpieczeństwa informacji - rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji

2. Administratorze danych osobowych - rozumie się przez to administratora danych - Uniwersytet Przyrodniczy w Lublinie reprezentowany przez Rektora,

3. Administratorze systemu informatycznego - rozumie się przez to wskazanego pracownika Ośrodka Informatyki Uniwersytetu Przyrodniczego w Lublinie,

4. Haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,

5. Identyfikatorze - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym, integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

6. Odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

   - osoby, której dane dotyczą
   - osoby upoważnionej do przetwarzania danych,
   - przedstawiciela, o którym mowa w art. 31 a ustawy,
   - podmiotu, o którym mowa w art. 31 ustawy,
   - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem

7. Osobie upoważnionej do przetwarzania danych osobowych - rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Rektora Uniwersytetu Przyrodniczego w Lublinie,

8. Poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

9. Przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy

10. Raporcie - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

11. Rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

12. Rozporządzeniu - rozumie się przez to 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 (DzU nr 100, poz. 1024),

13. Serwisancie - rozumie się przez to firmę zewnętrzną lub pracownika Ośrodka Informatyki zajmującego się sprzedażą instalacją, naprawą i konserwacją sprzętu komputerowego,

14. Sieci publicznej - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (DzU nr 73, poz. 852 ze zm.)

15. Sieci telekomunikacyjnej - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne,

16. Systemie informatycznym administratora danych - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

17. Teletransmisji - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

18. Ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2002 r. nr 101, poz. 926 ze zm.),

19. Uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

20. Użytkowniku - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło

III. Poziom Bezpieczeństwa

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.

IV. Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

Nadawanie i rejestrowanie uprawnień

1. 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 wniosek kierownika danej jednostki organizacyjnej.

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

3. Rejestracja użytkownika, o której mowa w pkt. 1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

4. Administrator systemu informatycznego albo upoważniony pracownik, o którym mowa w pkt. 2, przekazuje do zainteresowanej jednostki organizacyjnej informację o identyfikatorze, który został nadany użytkownikowi.

Wyrejestrowywanie uprawnień

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu informatycznego na wniosek kierownika jednostki organizacyjnej.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

    a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),

b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie:

   a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   b) -zawieszenia w pełnieniu obowiązków służbowych.

5. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:

   a) wypowiedzenie umowy o pracy,
   b) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.

6. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

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

Identyfikator

1. Identyfikator składa się co najmniej z sześciu znaków, z których przykładowo dwa pierwsze odpowiadają dwóm pierwszym literom imienia użytkownika, a cztery kolejne - czterem pierwszym literom jego nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne.

2. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu informatycznego , za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator, odstępując od zasady określonej w pkt 1.

Hasło użytkownika

1. Hasło powinno składać się z unikalnego zestawu co najmniej 6 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

2. System informatyczny wymusza zmianę hasła co 180 dni; administrator bezpieczeństwa informacji może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

3. 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.

Hasło administratora

1. Hasło administratora systemu przechowywane jest w zamkniętej kopercie w sejfie ognioodpornym, do którego ma dostęp administrator systemu informatycznego i administrator bezpieczeństwa informacji.

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

Tryb pracy na poszczególnych stacjach roboczych

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie, włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora.

2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika albo administratora bezpieczeństwa informacji.

3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd), wydruki leżące na biurkach oraz w otwartych szafach.

4. Monitory komputerów powinny mieć włączające się po 10 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.

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

6. Obowiązuje zakaz robienia kopii całych zbiorów danych; całe zbiory danych mogą być kopiowane tylko przez administratora systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.

7. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne 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.

8. Jednostkowe dane nie mogą być przekazywane pocztą elektroniczną pomiędzy komputerami administratora danych a komputerami przenośnymi użytkowników.

9. Zabronione jest przesyłanie danych osobowych pocztą elektroniczną.

10. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.

11. Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak by zapobiec ich utracie.

12. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie zasilającej.

13. 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.

14. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz. Klucz od pokoju przechowywany jest na portierni.

Tryb pracy na komputerach przenośnych

1. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na komputerach stacjonarnych.

2. Użytkownicy, którym zostały powierzone komputery przenośne, zobowiązani są chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.

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

4. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.

5. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 180 dni.

6. Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane i opatrzone hasłem dostępu.

7. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów, nawet w postaci zaszyfrowanej.

8. Użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na serwerze administratora danych, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.

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

10. Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatyczny system.

VII. Procedury tworzenia kopii zapasowych

1. W systemie informatycznym wykorzystującym technologię klient-serwer kopie zapasowe wykonuje się po stronie serwera.

2. Dostęp do kopii bezpieczeństwa ma tylko administrator systemu informatycznego oraz administrator bezpieczeństwa informacji.

3. Pozostałe kopie tworzy się na oddzielnych nośnikach informatycznych.

4. Nośniki zawierające kopie zapasowe należy oznaczać jako „Kopia zapasowa dzienna/tygodniowa/miesięczna" wraz z podaniem daty sporządzenia.

Częstotliwość wykonywania kopii

Kopie zapasowe tworzy się:

1. codziennie - na koniec dnia kopię wszystkich danych, które uległy zmianie tego dnia,

2. raz w tygodniu – na koniec tygodnia kopię wszystkich kluczowych aplikacji – pełną kopię.

3. raz w miesiącu - na koniec miesiąca kopię zarówno danych, jak i kluczowych aplikacji.

Testowanie kopii

5. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz na trzy miesiące poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.

Przechowywanie kopii

6. Kopie zapasowe przechowuje się w sejfie ognioodpornym administratora danych. Dostęp do kopii posiada wyłącznie administrator bezpieczeństwa informacji oraz administrator systemu i upoważnieni przez niego pracownicy. Każde wydanie i przyjęcie kopii jest odnotowywane w rejestrze depozytów.

7. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Jednocześnie kopie zapasowe muszą być odpowiednio zabezpieczone fizycznie (sejf ognioodporny w zabezpieczonym pomieszczeniu).

8. Kopie zapasowe mogą być przechowywane tylko w tych pomieszczeniach, w których jest zainstalowany system wykrywania pożaru.

9. Likwidacja nośników zawierających kopie

10. Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, taśmy, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.

11. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.

VIII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Zbiory danych przechowywane są domyślnie na serwerze obsługującym system informatyczny administratora danych. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze, przydzielonych każdemu użytkownikowi przez administratora systemu.

2. Zakazuje się przetwarzania danych osobowych na nośnikach zewnętrznych.

3. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.

4. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej instrukcji.

5. Nośniki 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.

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

IX. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez administratora systemu informatycznego lub upoważnionego pracownika Ośrodka Informatyki.

2. Oprogramowanie, o którym mowa w pkt 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w pkt 2, użytkownik komputera nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach,

administrator systemu informatycznego dokonuje sprawdzenia obecności wirusów na serwerach i stacjach roboczych jemu podległych.

4. Do obowiązków administratora systemu informatycznego należy zabezpieczenie funkcjonowania aktualizacji oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.

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

6. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko na stanowisku wydzielonym z sieci komputerowej administratora danych po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

7. Dostęp do internetu możliwy jest na wydzielonych stacjach roboczych, specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem firewall i translacją adresów NAT.

X. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

System informatyczny administratora danych umożliwia automatycznie:

1. przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,

2. sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do oprogramowania przetwarzającego dane osobowe (dotyczy to także komputerów przenośnych),

3. sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego:

    a) datę pierwszego wprowadzenia danych do systemu administratora danych,
    b) identyfikator użytkownika wprowadzającego te dane,
    c) źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą,
    d) nformacje o odbiorcach danych, którym dane osobowe zostały udostępnione,
    e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt. 8 ustawy.

4. Odnotowanie informacji, o których mowa w pkt. 3, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

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

1. Przeglądu i konserwacji systemu dokonuje administrator systemu informatycznego doraźnie.

2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) administrator systemu informatycznego dokonuje nie rzadziej niż raz na tydzień.

3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale administratora systemu informatycznego nie rzadziej niż raz na trzy miesiące.

4. Zapisy logów systemowych powinny być przeglądane przez administratora systemu informatycznego codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

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

XII. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym administratora danych przeprowadzane są - o ile to możliwe - przez pracowników Ośrodka Informatyki pod nadzorem administratora systemu informatycznego.

2. Naprawy i zmiany w systemie informatycznym administratora danych przeprowadzane przez serwisanta prowadzone są pod nadzorem administratora systemu w siedzibie administratora danych (jeśli to możliwe) lub poza siedzibą administratora danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

3. Nośnik danych (dysk, taśma, płyta lub inne), który zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie przy użyciu urządzenia niszczącego.

XIII. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

1. Użytkownik zobowiązany jest zawiadomić administratora bezpieczeństwa informacji lub uprzednio wskazanego przez niego pracownika ośrodka informatyki 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 lub dokumentów zawierających dane osobowe,
    h) zmianie położenia sprzętu komputerowego,
    i) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.
    j) zauważeniu innych anomalii pracy komputera

2. Do czasu przybycia na miejsce administratora bezpieczeństwa informacji lub pracownika ośrodka informatyki należy:

    a) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego 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 bezpieczeństwa informacji lub osoby przez niego wskazanej.

3. Pracownik ośrodka informatyki przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować administratora bezpieczeństwa informacji o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

4. Administrator bezpieczeństwa informacji po otrzymaniu zawiadomienia, o którym mowa w pkt. 1, powinien niezwłocznie:

   a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych, podjąć działania chroniące system przed ponownym naruszeniem,

   b) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego administratora danych, a następnie niezwłocznie przekazać jego kopię administratorowi danych.

5. Administrator bezpieczeństwa informacji w uzgodnieniu z administratorem systemu może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

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

7. Administrator danych po zapoznaniu się z raportem, o którym mowa w pkt. 4 lit. b, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego administratora danych bądź zastosowaniu środków ochrony fizycznej.

8. Administrator bezpieczeństwa informacji i administrator systemu informatycznego zobowiązani są do prowadzenia rejestru awarii systemu informatycznego przetwarzającego dane osobowe, zauważonych przypadkach naruszenia niniejszej instrukcji przez 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.

9. Administrator bezpieczeństwa informacji składa raz w roku administratorowi danych kompleksową analizę zarządzania systemem informatycznym.

XIV. Postanowienia końcowe

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

11. 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.

12. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.