Załącznik nr 2
do zarządzenia Rektora UŚ nr 9
z dnia 16 lutego 2016 r.

UNIWERSYTET ŚLĄSKI
W KATOWICACH

Egz. nr 0

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W UNIWERSYTECIE ŚLĄSKIM

K A T O W I C E
2016 rok

Spis treści

1. Cel instrukcji

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

2. Definicje

Ilekroć w niniejszej instrukcji jest mowa o:

1) ***administratorze danych*** osobowych - rozumie się przez to Uniwersytet Śląski reprezentowany przez Rektora decydującego o celach i środkach przetwarzania danych osobowych, w myśl art. 3 ustawy;
2) ***lokalnych administratorach danych osobowych*** - rozumie się przez to osoby, którym przekazano - odpowiednio do zakresu realizowanych przez nich celów statutowych - obowiązki i uprawnienia administratora danych osobowych w rozumieniu pkt. 2, ppkt. 1, niniejszej instrukcji;
3) ***pełnomocniku danych*** – rozumie się przez to Pełnomocnika Rektora ds. Danych Osobowych, któremu administrator danych osobowych powierzył nadzorowanie i koordynowanie zasad postępowania przy przetwarzaniu danych osobowych w Uniwersytecie Śląskim;
4) ***koordynatorze bezpieczeństwa informacji*** – rozumie się przez to osobę, której administrator danych osobowych powierzył pełnienie obowiązków koordynatora bezpieczeństwa *informacji;*
5) ***pełnomocnikach lokalnego administratora danych osobowych*** – rozumie się przez to osoby odpowiedzialne za nadzorowanie i koordynowanie zasad postępowania przy przetwarzaniu danych osobowych w jednostkach organizacyjnych Uczelni,
6) ***lokalnych koordynatorach bezpieczeństwa informacji*** – rozumie się przez to osoby, które realizują obowiązki koordynatora bezpieczeństwa informacji w jednostkach organizacyjnych Uczelni;
7) ***administratorze systemu*** – rozumie się przez to pracownika obsługującego systemy informatyczne, odpowiedzialnego za eksploatację systemu;
8) ***dysponencie systemu*** – rozumie się przez to kierownika jednostki organizacyjnej, odpowiedzialnego za eksploatację systemu;
9) ***haśle*** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
10) ***identyfikatorze*** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11) ***integralności danych*** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
12) ***odbiorcy danych*** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych,
    c) przedstawiciela, o którym mowa w art. 31a ustawy,
    d) podmiotu, o którym mowa w art. 31 ustawy,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są

udostępniane w związku z prowadzonym postępowaniem;

13) ***osobie upoważnionej do przetwarzania danych osobowych*** – rozumie się przez to osobę, która upoważniona została na piśmie do przetwarzania danych osobowych;
14) ***poufności danych*** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
15) ***pracowniku obsługującym systemy informatyczne*** – rozumie się przez to pracownika, zatrudnionego na stanowisku pracy o profilu informatycznym;
16) ***przetwarzającym*** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy;
17) ***raporcie*** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
18) ***rozliczalności*** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
19) ***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 (Dz. U. nr 100, poz. 1024);
20) ***sieci publicznej*** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.);
21) ***sieci telekomunikacyjnej*** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
22) ***serwisancie*** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;
23) ***systemie informatycznym administratora danych*** – rozumie się przez to sprzęt komputerowy, oprogramowanie i 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 osobowych;
24) ***teletransmisji*** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
25) ***ustawie*** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (jednolity tekst - Dz. U. z 2015 r. poz. 2135);
26) ***uwierzytelnianiu*** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
27) ***użytkowniku*** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

3. Poziom bezpieczeństwa

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

4. 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 polecenie dysponenta systemu.
2) Administrator systemu jest obowiązany upoważnić co najmniej jednego pracownika obsługującego systemy informatyczne 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 albo upoważniony pracownik, o którym mowa w pkt 2, przekazuje dysponentowi systemu informację o identyfikatorze, który został nadany użytkownikowi.

Wyrejestrowywanie uprawnień

1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na polecenie dysponenta systemu.
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 lub stałe zablokowanie konta użytkownika (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 pracę;
   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.

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

Identyfikator użytkownika

1) Celem stosowania identyfikatora jest jednoznaczne określenie osoby, która się nim posługuje. Identyfikator składa się:
   a) albo z sześciu znaków, z których pierwszy jest inicjałem imienia, drugi jest inicjałem nazwiska, a cztery kolejne to numer komputerowy pracownika;
   b) albo z ciągu znaków w postaci: imię.nazwisko@domena, gdzie „imię” jest imieniem pracownika, „nazwisko” jest nazwiskiem pracownika, a domena jest ciągiem znaków „us.edu.pl”.

c) dopuszczalne jest stosowanie innych konstrukcji identyfikatorów, pod warunkiem, że umożliwiają one jednoznaczną identyfikację osoby w systemie informatycznym.

2) W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, administrator systemu, za zgodą koordynatora bezpieczeństwa informacji, nadaje inny identyfikator, odstępując od zasady określonej w pkt 1, lit. a), b).
3) W identyfikatorach pomija się polskie znaki diakrytyczne.

Hasło użytkownika

1) Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu 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 30 dni; koordynator 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

Hasło administratora systemu przechowywane jest w zamkniętej kopercie w sejfie ognioodpornym, do którego mają dostęp wyłącznie dysponent systemu i administrator systemu.

6. 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 koordynatora bezpieczeństwa informacji.
3) Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach.
4) Monitory komputerów wyposażone są we 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 mogą być przekazywane pocztą elektroniczną pomiędzy komputerami administratora danych osobowych, a komputerami przenośnymi użytkowników tylko po ich zaszyfrowaniu.
9) Przesyłanie danych osobowych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.
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.
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.
15) Klucze od pokoi pobierane są z portierni, przez osoby upoważnione, za podpisem w „Książce wydawanych kluczy”.

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, powinni 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 30 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 osobowych, 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, 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.
10) Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.

7. Procedury tworzenia kopii zapasowych

1) W systemie informatycznym wykorzystującym technologię użytkownik-serwer kopie zapasowe wykonuje się po stronie serwera.
2) Dostęp do kopii bezpieczeństwa mają tylko pracownicy obsługujący systemy informatyczne.
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 aplikacji;
3) raz w miesiącu – na koniec miesiąca kopię zarówno danych, jak i aplikacji, w tym także systemu operacyjnego.

Testowanie kopii

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

Przechowywanie kopii

1) Kopie zapasowe przechowuje się w sejfie ognioodpornym administratora danych osobowych. Dostęp do kopii posiada wyłącznie koordynator bezpieczeństwa informacji oraz administrator systemu i upoważnieni przez niego pracownicy. Każde wydanie i przyjęcie kopii jest odnotowywane w rejestrze depozytów.
2) 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).
3) Kopie zapasowe mogą być przechowywane tylko w tych pomieszczeniach, w których jest zainstalowany system wykrywania pożaru.

Likwidacja nośników zawierających kopie

1) 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,

dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.

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

8. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1) Zbiory danych przechowywane są generalnie na serwerze obsługującym system informatyczny administratora danych osobowych. 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 zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.
3) Na nośnikach, o których mowa w pkt 2, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
4) 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.
5) 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.
6) 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.
7) Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

9. 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.
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, administrator systemu nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
4) Do obowiązków administratora systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
5) Użytkownik jest obowiązany zawiadomić administratora systemu 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 osobowych, po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
7) Dostęp do Internetu możliwy jest wyłącznie na stacjach roboczych, specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem Firewall i translacją adresów NAT.

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

System informatyczny administratora danych osobowych umożliwia automatycznie:

1) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
2) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (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 osobowych,
   b) identyfikator użytkownika wprowadzającego te dane,
   c) źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą,
   d) informacje o odbiorcach danych, którym dane osobowe zostały udostępnione,
   e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

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

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

1) Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.
2) Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) administrator systemu dokonuje nie rzadziej niż raz na tydzień.
3) Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale administratora systemu nie rzadziej niż raz na miesiąc.
4) Zapisy logów systemowych powinny być przeglądane przez administratora systemu codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
5) Kontrole i testy przeprowadzane przez koordynatora bezpieczeństwa informacji powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

12. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1) Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym administratora danych osobowych przeprowadzane są – o ile to możliwe – przez pracowników pionu informatyki administracji ogólnouczelnianej pod nadzorem administratora systemu.
2) Naprawy i zmiany w systemie informatycznym administratora danych osobowych przeprowadzane przez serwisanta prowadzone są pod nadzorem administratora

systemu w siedzibie administratora danych osobowych (jeśli to możliwe) lub poza siedzibą administratora danych osobowych, 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) Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce.

13. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

1) Użytkownik zobowiązany jest zawiadomić koordynatora bezpieczeństwa informacji lub uprzednio wskazanego przez niego pracownika obsługującego systemy informatyczne 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.
2) Do czasu przybycia na miejsce koordynatora bezpieczeństwa informacji lub wskazanego przez niego pracownika obsługującego systemy informatyczne 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 koordynatora bezpieczeństwa informacji lub osoby przez niego wskazanej.
3) Pracownik obsługujący systemy informatyczne przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować koordynatora bezpieczeństwa informacji o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.
4) Koordynator 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,
b) podjąć działania chroniące system przed ponownym naruszeniem,
c) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego administratora danych osobowych, a następnie niezwłocznie przekazać jego kopię administratorowi danych osobowych.

5) Koordynator 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 osobowych, po zapoznaniu się z raportem, o którym mowa w pkt 4 lit. c, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego administratora danych osobowych bądź zastosowaniu środków ochrony fizycznej.
8) Koordynator bezpieczeństwa informacji i administrator systemu zobowiązani są do informowania administratora danych osobowych, o awariach systemu informatycznego, 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) Koordynator bezpieczeństwa informacji składa raz w roku administratorowi danych osobowych kompleksową analizę zarządzania systemem informatycznym.

14. Postanowienia końcowe

1) W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2) 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.
3) 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.