Załącznik nr 2 do zarządzenia
Rektora Powiślańskiej Szkoły Wyższej w Kwidzynie
Z dnia 30.09.2008 r.

INSTRUKCJA

ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W POWIŚLAŃSKIEJ SZKOLE WYŻSZEJ W KWIDZYNIE

Dokumenty powiązane:

Polityka bezpieczeństwa przetwarzania danych osobowych w Powiślańskiej Szkole Wyższej w Kwidzynie

§ 1

Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w PSW w Kwidzynie, zwana dalej „Instrukcją" określa zasady, tryb postępowania i zalecenia Administratora Danych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
2. 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).
3. Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.
4. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.
5. Administrator Bezpieczeństwa Informacji powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe. Nie oznacza to automatycznego prawa dostępu do danych osobowych przetwarzanych w tych systemach.

§ 2

Obowiązki w zakresie ochrony danych osobowych

1. Do obowiązków osób zaangażowanych w przetwarzanie danych osobowych w systemach informatycznych należy:
   1) Podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.
   2) Przetwarzanie danych osobowych wyłącznie w celach określonych przez swoich przełożonych.
2. Do kompetencji osób zarządzających pracownikami należy w szczególności wystawianie dla bezpośrednio podległych pracowników wniosków o nadanie, zmianę lub cofnięcie uprawnień do systemów informatycznych, w których są przetwarzane dane osobowe.
3. Użytkownicy powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§ 3

Obowiązki Administratora Bezpieczeństwa Informacji

Do obowiązków Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Nadzór nad stosowaniem środków ochrony.
2) Nadzór nad przestrzeganiem przez Administratorów Systemów i użytkowników systemu procedur bezpieczeństwa.
3) Wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków.
4) Prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, stanowiącej część ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i stopień ochrony danych osobowych w PSW w Kwidzynie.
5) Kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.
6) Prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych.
7) Uzgadnianie z właściwymi Administratorami Systemów szczególnych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych.
8) Zapewnienie doradztwa w zakresie przestrzegania przez pracowników firmy zewnętrznej zasad ochrony danych osobowych przyjętych w PSW w Kwidzynie.

§ 4

Obowiązki Administratorów Systemu

Do obowiązków Administratorów Systemu w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę

   danych osobowych w nich przetwarzanych.
2) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3) Kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym.
4) Zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną.
5) Utrzymanie systemu w należytej sprawności technicznej.
6) Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.
7) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

§ 5

Obowiązki Właścicieli zasobów danych osobowych

Do obowiązków Właścicieli zasobów danych osobowych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Zapewnienie właściwego poziomu ochrony danych osobowych w systemach, dla danych za które są odpowiedzialni.
2) Informowanie Administratora Bezpieczeństwa Informacji o zmianie celu przetwarzania danych osobowych w systemie lub poszerzeniu zakresu zbieranych danych osobowych.

§ 6

Obowiązki użytkowników

Do obowiązków użytkowników systemu informatycznego w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności

1) Przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych.
2) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3) Udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania.
4) Uniemożliwienie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych.
5) Informowanie Administratora Bezpieczeństwa Informacji o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.
6) Wykonywania bez zbędnej zwłoki poleceń Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

§ 7

Bezpieczna eksploatacja systemów informatycznych

Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe zostaje zapewniona poprzez przestrzeganie następujących zasad:

1) Użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie.
2) Użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych.
3) Użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania.
4) Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.
5) Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.

6) Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera.

7) Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.

8) Nieautoryzowane podłączenie własnego lub strony trzeciej urządzenia teleinformatycznego do systemu informatycznego xxxxxx jest zabronione.

§8

Nadawanie uprawnień do przetwarzania danych osobowych

1. Użytkownicy systemu przetwarzającego dane osobowe przed przystąpieniem do przetwarzania danych osobowych w tym systemie informatycznym, zobowiązani są zapoznać się z:
   1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.).
   2) Polityką bezpieczeństwa przetwarzania danych osobowych w PSW w Kwidzynie.
   3) Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.
2. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o:
   1) Zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami.
   2) Uzyskanie formalnego upoważnienia do przetwarzania danych osobowych.
3. Wzory oświadczenia oraz upoważnienia stanowią załączniki nr 1 i 2 do „Polityki bezpieczeństwa przetwarzania danych osobowych w PSW w Kwidzynie”
4. Po spełnieniu wymagań określonych w ust. 3, przełożony pracownika albo ABI, w przypadku, gdy dostęp do danych osobowych przetwarzanych w systemie ma uzyskać Rektor, zgłasza wniosek do Administratora Systemu Informatycznego (ASI) o zarejestrowanie użytkownika w systemie (założenie mu konta). Wniosek przekazany do ASI może być przekazany w postaci elektronicznej, ale w takim wypadku konieczna jest jego archiwizacja na odpowiednich nośnikach gwarantujących trwałość i niezmienność zapisu
5. Identyfikator oraz zakres dostępu użytkownika powinien być rejestrowany w ewidencji osób upoważnionych do przetwarzania danych osobowych, określonej w §16 „Polityki bezpieczeństwa przetwarzania danych osobowych w PSW w Kwidzynie”
6. Administratorzy Systemu powinni przekazywać użytkownikom tymczasowe hasła dostępowe w sposób bezpieczny. W tym celu powinni unikać pośrednictwa osób trzecich lub korzystania do tego celu z niechronionych wiadomości poczty elektronicznej.
7. Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach należy stosować odpowiednio, w przypadku zmiany uprawnień w systemach lub w przypadku odebrania uprawnień w systemach.
8. Zmiany dotyczące użytkownika, takie jak rozwiązanie umowy o pracę lub utrata upoważnienia, są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu oraz unieważnienia hasła i odnotowanie tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w ust. 6.
9. Prawa dostępu przyznane użytkownikom, którzy nie są pracownikami etatowymi PSW w Kwidzynie powinny mieć charakter czasowy i mogą być przyznawane na okres odpowiadający wykonywanemu zadaniu.

10. Dostęp do systemu informatycznego a także do poszczególnych aplikacji i baz danych przetwarzających dane osobowe powinien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła.

§ 9

Metody i środki uwierzytelniania w systemie

1. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.
2. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
   1) Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku.
   2) Hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi z zastrzeżeniem § 8 ust. 7
   3) Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie.
   4) Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności.
   5) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).
3. Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.
4. Administratorzy Systemu są odpowiedzialni za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.
5. Administratorzy Systemu powinni przeprowadzać przegląd autoryzacji i uprawnień nie rzadziej niż co 6 miesięcy dla standardowych użytkowników oaz co 3 miesiące dla użytkowników posiadających specjalne przywileje – przegląd powinien być dokumentowany.

§ 10

Wymogi dotyczące uwierzytelniania

1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Administratora Bezpieczeństwa Informacji sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

5. Hasło początkowe, które jest przydzielane przez Administratora Systemu, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika.
6. Użytkownicy powinny wybierać hasła dobrej jakości:
   1) Długości co najmniej 8 znaków.
   2) Które są łatwe do zapamiętania, a trudne do odgadnięcia.
   3) Nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.).
   4) W których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny.
   5) W których nie występują kolejne znaki, które nie są topologiczne (tzn. wynikające z układu klawiszy na klawiaturze, typu „qwer6", „zaq1xsw2CDE#" itp.).
7. Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.
8. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
9. Należy unikać ponownego lub cyklicznego używania starych haseł.
10. Hasła dla użytkowników o wysokich uprawnieniach (np. root, administrator) mogą być wykorzystywane tylko w uzasadnionych przypadkach i fakt ten powinien być udokumentowany.
11. Hasła użytkowników o wysokich uprawnieniach powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
12. Rutynowe działania użytkownika nie powinny być prowadzone z wykorzystaniem kont uprzywilejowanych.
13. Udostępnienie hasła osobie postronnej należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

§ 11

Wymogi dotyczące zmiany haseł

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
   1) Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).
   2) W przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do właściwego Administratora Systemu, w sytuacji:
   1) Zapomnienia/zgubienia hasła.
   2) Wygaśnięcia ważności hasła.
   3) Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.
   4) Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.
3. Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

§ 12

Procedura bezpiecznego uwierzytelniania

1. Procedura bezpiecznego uwierzytelniania w systemie informatycznym zapewnia minimalizowanie możliwości nieautoryzowanego dostępu do systemu. Procedura powinna ujawniać minimum informacji o systemie informatycznym tak, aby nie pozwolić nieuprawnionemu użytkownikowi na uzyskanie dodatkowych wskazówek w celu ich wykorzystania w sposób niedozwolony. W tym celu należy zapewnić:
   1) Wyświetlanie ogólnego ostrzeżenia, że dostęp do stacji roboczej dozwolony jedynie dla uprawnionych użytkowników.
   2) Zatwierdzanie jedynie kompletnych informacji wejściowych, niezbędnych przy logowaniu jeżeli wystąpi błąd, system nie powinien wskazywać, która część danych jest poprawna, a która niepoprawna.
   3) Ograniczenie liczby nieudanych prób logowania się do systemu, np. do trzech prób, oraz uwzględnić:
      a. wykonywanie zapisu nieudanych i udanych prób,
      b. wymuszanie odstępu czasowego przed każdą kolejną próbą logowania się lub odrzucanie wszelkich dalszych prób, jeśli nie mają specjalnej autoryzacji,
      c. rozłączenie połączeń,
      d. wysłanie wiadomości alarmowej na konsolę systemową w przypadku, gdy maksymalna liczba prób została osiągnięta,
      e. ustawienia maksymalnej liczby prób logowania się w połączeniu z minimalną długością hasła oraz wartością chronionego systemu,
      f. ograniczenie maksymalnego i minimalnego czasu trwania logowania; jeśli zostanie on przekroczony, system powinien przerwać procedurę logowania,
   4) Wyświetlanie następujących informacji po pomyślnym zalogowaniu:
      a. datę i czas ostatniego pomyślnego logowania do systemu,
      b. szczegółowe dane dotyczące nieudanych prób logowania się, jakie zdarzyły się od chwili ostatniej udanej próby,
   5) Blokowanie wyświetlania hasła w trakcie wprowadzania lub ukrywanie wprowadzanych znaków pod symbolami.
   6) Blokowanie przesyłania haseł przez sieć jawnym tekstem.

§ 13

Wymagania dotyczące sprzętu i oprogramowania

1. Wygaszacz stacji roboczej powinien być skonfigurowany w taki sposób, aby aktywował się automatycznie po upływie 10 minut od ostatniego użycia stacji roboczej, uruchamiając blokadę stacji roboczej, wymuszającą ponowne zalogowanie.
2. Ekrany monitorów należy ustawić w taki sposób, by uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.
3. Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

4. Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freewere, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty Administratorów Systemu.
5. Przed zainstalowaniem nowego oprogramowania właściwy Administrator Systemu lub inna upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
6. Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.
7. Serwer systemu przetwarzającego dane osobowe powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak aby przed ostatecznym zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.
8. Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
9. Gniazda zasilania sieci teleinformatycznej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników i wykonane w specjalnym standardzie.
10. Wdrażanie aplikacji i oprogramowania eksploatowanych systemów powinno być poprzedzone wyczerpującymi, pozytywnymi i udokumentowanymi testami.
11. Powinna zostać opracowana metoda przywracania poprzedniej wersji, zanim zmiany zostaną wdrożone.
12. Należy przechowywać wszystkie poprzednie wersje oprogramowania jako środek utrzymania ciągłości działania.
13. Należy zapewnić rejestrowanie wszystkich błędów, związanych z problemami przetwarzania danych osobowych, zgłaszanych przez użytkowników lub programy systemowe.
14. Należy zapewnić ograniczenie dostępu do bibliotek źródłowych programów a dostęp i zmiany odnotowywać.
15. Należy chronić informacje zawarte w dziennikach zdarzeń systemów przed manipulacją i nieautoryzowanym dostępem.
16. Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.
17. Należy zapewnić aby porty i usługi, które nie są wykorzystywane były zablokowane.

§ 14

Funkcjonalność systemu informatycznego

1. System informatyczny służący do przetwarzania danych osobowych powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.
2. W przypadku zbierania danych osobowych od osoby, której dane nie dotyczą należy zapewnić w systemie informatycznym odnotowywanie informacji o źródle pochodzenia danych. Proces ten nie musi odbywać się automatycznie.
3. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie w bazie danych tego systemu informacji,

komu, kiedy i w jakim zakresie dane zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.

4. W przypadku zgłoszenia sprzeciwu o którym mowa w art. 32 ust 1 pkt. 8 Ustawy, wobec przetwarzania danych osobowych system powinien zapewniać odnotowywanie tej informacji.
5. Należy zapewnić dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenie i wydrukowanie:
   1) Zestawień zakresu i treści przetwarzanych na jej temat danych osobowych.
   2) Zestawienia zawierającego informacje wymagane w § 7 ust. 1 Rozporządzenia.
6. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach, wymagania, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia, mogą być realizowane w jednej z nich lub w odrębnej aplikacji przeznaczonej do tego celu.
7. Treść ostatecznego rozstrzygnięcia indywidualnej sprawy osoby, której dane dotyczą, nie może być wyłącznie wynikiem operacji na danych osobowych, prowadzonych w aplikacji lub systemie informatycznym.
8. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne
9. Zaleca się wbudowanie do aplikacji funkcjonalności, zapewniających wymuszanie zmiany haseł po zadanym czasie, badania ich długości, jakości i powtarzalności (z użyciem funkcji skrótu).

§ 15

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest postępować zgodnie z procedurą opisaną w §8 „Polityki bezpieczeństwa przetwarzania danych osobowych w PSW w Kwidzynie”
3. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zablokować swoją stację roboczą poprzez wciśnięcie klawiszy “ctrl+alt+delete” i wybranie opcji “Zablokuj stację roboczą”.
4. Kończąc pracę, użytkownik obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz wymiennych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich zamykanych szafkach.

§ 16

Przetwarzanie, udostępnianie i likwidacja danych osobowych

1. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
   1) Ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi.
   2) Stosowanie metod kryptograficznych.

3) Stosowanie odpowiednich zabezpieczeń fizycznych.

4) Stosowanie odpowiednich zabezpieczeń organizacyjnych.

W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

2. Nieuzasadnione kopiowanie przez użytkowników plików z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji jest zabronione bez akceptacji ze strony Administratora Bezpieczeństwa Informacji.
3. W przypadku udostępniania danych osobowych odbiorcy danych w rozumieniu art. 7 pkt 6 Ustawy, użytkownik ma obowiązek odnotować komu i kiedy udostępniono poszczególne dane.
4. Jeżeli dane osobowe nie są pozyskane od osoby, której dotyczą, użytkownik zobowiązany jest odnotować w systemie informatycznym źródło pochodzenia danych.
5. W przypadku zgłoszenia sprzeciwu o którym mowa w art. 32 ust 1 pkt. 8 Ustawy, wobec przetwarzania danych osobowych użytkownik usuwa z systemu dane osoby zgłaszającej sprzeciw pozostawiając jedynie imię, nazwisko i ew. nr PESEL. W przypadkach wątpliwych użytkownik konsultuję się z Administratorem Bezpieczeństwa Informacji.
6. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych nie podlegających archiwizacji w odrębnym trybie dla którego cel przetwarzania ustał, Administrator Bezpieczeństwa Informacji lub osoby upoważnione sporządzają protokół, w którym zamieszczają następujące informacje:

   1) Datę dokonania likwidacji.

   2) Przedmiot likwidacji (aplikacja, baza).

   3) Podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

7. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują Właściciele zasobów danych osobowych.
8. W przypadku likwidacji elektronicznych nośników informacji, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych.
9. Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika dane osobowe.

§ 17

Kopie zapasowe

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane na bieżąco przez Administratorów Systemu.
2. Kopie zapasowe powinny być tworzone na nośnikach magnetycznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych a każdy proces wykonywania kopii zapasowej powinien być dokumentowany.
3. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.
4. W celu usystematyzowania procesu wykonywania kopi zapasowej, odpowiedzialni za ten proces Administratorzy Systemu są zobowiązani do sporządzenia harmonogramu wykonywania kopi zapasowej wraz z opisem narzędzi służących do jej wykonywania, nazwą polityk, nazwą systemu, nazwą bazy danych, terminem okresu przechowywania, rodzajem wykorzystywanego nośnika wraz z numerem seryjnym nośnika.

5. Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez Administratorów Systemu, z uwzględnieniem niniejszych postanowień.
6. Administratorzy Systemu odpowiedzialni za tworzenie kopi zapasowych zobowiązani są przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach pod kątem ewentualnej przydatności w sytuacji awarii systemu.
7. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie Administratorowi System oraz Administratorowi Bezpieczeństwa Informacji.
8. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez Administratora Systemu.
9. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu.
10. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonują Administratorzy Systemu lub inna upoważniona przez Rektora osoba.
11. Proces niszczenia kopii zapasowych powinien odbywać się komisyjnie i powinien być dokumentowany.

§ 18

Przechowywanie nośników elektronicznych zawierających dane osobowe

1. Dane osobowe mogą być przechowywane:
   1) Na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych.
   2) Na wymiennych nośnikach elektronicznych.
2. Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.
3. Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników.
4. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.
5. Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.
6. Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej, ognioodpornej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione.
7. Nośniki magnetyczne i optyczne z danymi osobowymi powinny być:
   1) Oznaczane i przechowywane w zamykanych szafach lub sejfach.
   2) Przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Bezpieczeństwa Informacji.
8. Informację o maksymalnym okresie przechowywania nośników magnetycznych oraz optycznych, na których zapisane są dane osobowe przekazują Właściciele zasobów danych osobowych do Administratora Bezpieczeństwa Informacji.

§ 19

Ochrona systemu informatycznego przed działaniem szkodliwego oprogramowania

1. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.
3. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
5. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują Administratorzy Systemu niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.
6. W razie zainfekowania systemu Administratorzy Systemu odpowiadają za usunięcie wirusa.
7. Administratorzy Systemu mają prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

§ 20

Zasady komunikacji w sieci teleinformatycznej

1. Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
2. Pliki zawierające dane osobowe mogą się znajdować jedynie na serwerach, gdzie podlegają ochronie zapewnianej przez mechanizmy bezpieczeństwa systemu operacyjnego.
3. Wyłącznie w sytuacjach wyjątkowych dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdującą się w określonym systemie informatycznym.
4. Zgodę na przetwarzanie danych w sytuacjach określonych w ust. 3 wydają Właściciele zasobów danych osobowych.
5. 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.
6. Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane a logi połączeń archiwizowane w trybie ciągłym i bezterminowym.
7. System informatyczny służący do przetwarzania danych osobowych, Administratorzy Systemu powinni chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
8. Zabezpieczenia logiczne, o których mowa w ust. 7 powyżej, obejmują:
   1) Kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną.
   2) Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
9. Kontrola powinna być nadzorowana przez Administratorów Systemu a jej wynik powinien być dokumentowany w dziennikach pracy Administratorów Systemu.

10. Zdalne uruchamianie komend systemowych ze stacji roboczych znajdujących się w lokalizacjach nie należących do PSW w Kwidzynie jest możliwe, po prawidłowym logowaniu się użytkownika i zastosowaniu „silnego” uwierzytelnienia.

§ 21

Zasady monitorowania, przeglądu i konserwacji systemu informatycznego

1. Przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu wymagają obecności Administratora Systemu lub innej wyznaczonej osoby.
2. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemach odpowiadają Administratorzy Systemu.
3. W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia w rozumieniu art. 31 ustawy o ochronie danych osobowych.
4. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
5. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować: poprawność działania wszystkich elementów aplikacji, poprawność funkcjonalną systemu.
6. Każda zmiana parametrów systemu służącego do przetwarzania danych osobowych powinna być dokładnie dokumentowana.
7. Codziennie Administratorzy Systemu powinni przeprowadzać kontrolę logów zdarzeń zachodzących w systemie.
8. Raz do roku należy przeprowadzać weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich stacjach roboczych podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa.
9. Czynności wymienione w ust. 7 i 8 powyżej, powinny być dokumentowane w dziennikach pracy Administratorów Systemu.

§ 22

Zasady postępowania z komputerami przenośnymi

1. Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.
2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:
   1) Stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym.
   2) Zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego - identyfikator i hasło.
   3) Nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.

4) Nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej.

5) Zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią PSW w Kwidzynie należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.
4. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.
5. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

§ 23

Postanowienia końcowe

1. Administrator Bezpieczeństwa Informacji zobowiązany jest zapoznać z treścią Instrukcji każdego użytkownika systemu informatycznego służącego do przetwarzania danych osobowych.
2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisów wykonawczych do tej Ustawy.