PAŃSTWOWA
WYŻSZA SZKOŁA INFORMATYKI
I PRZEDSIĘBIORCZOŚCI
w Łomży
18-400 Łomża, ul. Akademicka 14
tel. 86/ 215 59 50

Załącznik Nr 2 do zarządzenia Nr 66/15 Rektora
Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży
z dnia 29.10.2015 r. *w sprawie* ochrony danych osobowych w PWSIiP w Łomży

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży

Spis treści

1. Wstęp

1.1. Instrukcja stanowi zestaw procedur opisujących zasady zabezpieczania danych osobowych przetwarzanych w systemach informatycznych Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży.

1.2. Instrukcję opracowano na podstawie Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r., poz 1182 z późn. zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

1.3. Ilekroć w instrukcji jest mowa o:

1) Ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej Ustawą;
2) PWSIiP, Uczelni – rozumie się przez Państwową Wyższą Szkołę Informatyki i Przedsiębiorczości w Łomży;
3) Zbiorze danych, zbiorze – rozumie się przez to zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów;
4) Administratorze Danych Osobowych, ADO – rozumie się przez to Rektora Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży, decydującego o celach i środkach przetwarzania danych osobowych;
5) Administratorze Bezpieczeństwa Informacji, ABI – rozumie się przez to osobę powołaną przez ADO na podstawie Ustawy, odpowiedzialną za organizację ochrony danych osobowych;
6) Administratorze Systemu Informatycznego, ASI – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagające specjalnych uprawnień;
7) Kierowniku komórki organizacyjnej – należy przez to rozumieć kierowników jednostek i komórek organizacyjnych, w których zatrudnieni są pracownicy przetwarzający dane osobowe;
8) Polityce bezpieczeństwa – rozumie się przez to dokument określający politykę ochrony danych osobowych w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży, rejestrowanych w zbiorach papierowych oraz w systemach informatycznych;
9) Identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
10) Haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

11) Sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
12) Raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
13) Uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
14) 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 osobowych,
    c) wyznaczonego przez Administratora Danych Osobowych przedstawiciela w Rzeczypospolitej Polskiej, w przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim,
    d) podmiotu któremu powierzono przetwarzanie danych,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

1.4. Instrukcję stosuje się do wszystkich systemów komputerowych służących do przetwarzania danych osobowych w Uczelni.

1.5. Dla poszczególnych systemów komputerowych mogą być sporządzane dodatkowe szczegółowe instrukcje zarządzania.

2. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

2.1. Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych.

2.2. Upoważnienia nadaje i odwołuje Administrator Bezpieczeństwa Informacji na podstawie wniosku kierownika właściwej komórki organizacyjnej, kierownika/koordynatora projektu, kierownika pionu organizacyjnego lub Kierownika Biura Rektora. Wzór wniosku stanowi Załącznik Nr 1 do Instrukcji. Wykaz programów służących do przetwarzania danych osobowych wraz ze wskazaniem administratorów stanowi Załącznik nr 3 do Polityki Bezpieczeństwa Ochrony Danych Osobowych w PWSIiP w Łomży.

2.3. Przed nadaniem upoważnienia, ABI zobowiązany jest do sprawdzenia, czy osoba upoważniona:

1) odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych lub została zapoznana z Polityką Bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym,
2) podpisała oświadczenie o zachowaniu poufności,
3) będzie przetwarzać dane osobowe w zakresie i celu określonym w upoważnieniu.

2.4. W przypadku zmiany stanowiska pracy, wydanie nowego upoważnienia jest konieczne, jeżeli zmianie ulega zakres i cel przetwarzania danych przez pracownika posiadającego upoważnienie.

2.5. Upoważnienie, bądź jego odwołanie sporządzane są na piśmie w trzech egzemplarzach – dla osoby upoważnionej, do akt osobowych pracownika oraz dla ABI. Wzór upoważnienia/odwołania upoważnienia stanowią Załączniki Nr 2 i Nr 3 do Instrukcji.

2.6. W sytuacjach wyjątkowych (np. stan zagrożenia dla ochrony danych osobowych, nieobecność ABI) upoważnienie może odwołać kierownik komórki organizacyjnej, kierownik/koordynator projektu, kierownik pionu organizacyjnego lub Kierownik Biura Rektora. Decyzja kierownika wymaga akceptacji ABI, dokonanej w najbliższym możliwym terminie.

2.7. Wydane upoważnienia do przetwarzania danych osobowych oraz ich odwołanie, rejestrowane są w rejestrze osób upoważnionych do przetwarzania danych osobowych. Wzór rejestru osób upoważnionych do przetwarzania danych osobowych stanowi Załącznik Nr 4 do Instrukcji. Rejestr osób upoważnionych prowadzi ABI.

2.8. Czynności konfiguracyjne związane z przydzieleniem lub odebraniem praw do zbioru danych, lub programów do przetwarzania danych wykonuje administrator właściwego systemu informatycznego na podstawie przedstawionego upoważnienia/odwołania upoważnienia, lub rejestru osób upoważnionych.

3. Stosowane metody i środki uwierzytelniania

3.1. Podstawową metodą uwierzytelniania użytkowników w systemach komputerowych służących do przetwarzania danych osobowych są konta użytkowników. Konto składa się z identyfikatora użytkownika i hasła. W zależności od systemu dla danego konta można stosować zamiennie identyfikatory użytkownika (np. adres e-mail, numer indeksu, PESEL) z zachowaniem kontroli właściwego hasła.

3.2. Identyfikator użytkownika jest jawny i może być nadawany przez administratora właściwego systemu informatycznego indywidualnie, generowany automatycznie lub wyznaczany na podstawie zapisanych danych użytkownika (np. adres email, nr indeksu), w zależności od specyfiki systemu komputerowego i uwierzytelniania użytkowników.

3.3. Identyfikator użytkownika, który stracił prawo do przetwarzania danych, należy niezwłocznie zablokować lub zmodyfikować uprawnienia w taki sposób, aby przetwarzanie nie było możliwe w systemie, do którego odwołano uprawnienia.

3.4. Ważność identyfikatora użytkownika w systemie służącym do przetwarzania danych, może być określana przez ASI na podstawie informacji zawartych na upoważnieniu, lub na podstawie danych kadrowych, tj. dacie rozpoczęcia i zakończenia umowy o pracę lub zlecenia.

3.5. W przypadku utraty uprawnień użytkownika do przetwarzania danych, w/w identyfikatora nie można przydzielać innej osobie.

3.6. Hasło użytkownika powinno spełniać następujące wymagania:

1) hasło nie może być jednakowe z identyfikatorem użytkownika i nie może zawierać danych personalnych (np. imienia, nazwiska, daty urodzenia użytkownika),
2) hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
3) hasło musi być unikalne i nie powinno być powtarzane.

3.7. Hasło nie może być wyświetlane na ekranie w trakcie wpisywania. Użytkownik zobowiązany jest do zachowania hasła w tajemnicy, również po ustaniu jego ważności.

3.8. Hasło użytkownika musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana nie jest w tym czasie możliwa, to należy wykonać ją w najbliższym możliwym terminie. Zasada ta nie dotyczy kont systemowych służących do automatycznej wymiany danych między systemami.

3.9. W sytuacjach wyjątkowych (np. zastępstwa z powodu urlopu lub choroby) hasło użytkownika może być, na wniosek przełożonego oraz po akceptacji ABI, dokonanej w najbliższym możliwym terminie, udostępnione innej osobie pod warunkiem, że osoba której udostępniane jest hasło, posiada odpowiednie upoważnienie do przetwarzania określonych danych. Wzór wniosku o udostępnienie hasła stanowi Załącznik Nr 5 do Instrukcji. Po ustaniu sytuacji wyjątkowej użytkownik, który udostępnił hasło musi niezwłocznie je zmienić.

3.10. Hasła głównych kont systemowych, kont administracyjnych, interfejsów wymiany danych mogą być znane administratorom systemu i mają oni obowiązek zachowania ich w tajemnicy.

3.11. W przypadku złamania poufności hasła, użytkownik zobowiązany jest do jego natychmiastowej zmiany oraz do zgłoszenia tego faktu ABI oraz ASI.

3.12. W przypadku, gdy użytkownik zapomniał hasła, powinien:

1) samodzielnie wykonać procedurę resetowania hasła pod warunkiem, że aplikacja udostępnia taką funkcjonalność i istnieje możliwość dodatkowej weryfikacji tożsamości użytkownika,
2) zgłosić się do właściwego ASI w celu zresetowania hasła. Hasło wpisane przez ASI powinno być niezwłocznie zmienione przez użytkownika.

3.13. Zabrania się przesyłania haseł jawnym tekstem w wiadomościach e-mail.

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

4.1. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń (np. otwarta obudowa komputera,

podłączone nieznane nośniki danych lub urządzenia). W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić przełożonego lub ABI. W przypadku stwierdzenia naruszenia zasad ochrony danych osobowych należy postępować zgodnie z zasadami opisanymi w pkt. 9 Polityki Bezpieczeństwa.

4.2. Przed rozpoczęciem przetwarzania danych użytkownik powinien upewnić się, że ustawienie monitora nie pozwala na wgląd w wyświetlane treści przez osoby postronne oraz, że żadna inna osoba przebywająca w pomieszczeniu nie jest w stanie podejrzeć wpisywanego na klawiaturze hasła.

4.3. Podczas użytkowania aplikacji dostępnych za pomocą przeglądarki internetowej, przed podaniem identyfikatora użytkownika i hasła należy upewnić się, że włączone jest szyfrowanie połączenia internetowego (np. sprawdzenie czy adres zaczyna się od zapisu „https://"). W przypadku wątpliwości należy wstrzymać się z wpisywaniem jakichkolwiek danych i skontaktować się z administratorem właściwego systemu informatycznego.

4.4. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych, z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika, z wyjątkiem sytuacji szczególnych (urlop, choroba), lub kiedy zachodzi potrzeba wglądu w zasoby plikowe zapisane w profilu określonego użytkownika oraz przełożony lub ABI wyrazili na to zgodę.

4.5. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych oraz wylogować się z systemu operacyjnego, lub włączyć wygaszasz ekranu chroniony hasłem. Zabrania się pozostawiania otwartych dokumentów na ekranie monitora.

4.6. Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone uruchomieniem procedur zapisujących zmodyfikowane dane, zamknięciem używanych aplikacji i odłączeniem przenośnych nośników optycznych i elektronicznych używanych w czasie pracy. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następuje poprzez wylogowanie się z systemu operacyjnego lub wyłączenie komputera.

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

5.1. Kopie zapasowe zbiorów danych osobowych przetwarzanych w Uczelni wykonywane są automatycznie za pomocą oprogramowania do wykonywania kopii zapasowych (w przypadku systemów Windows) oraz skryptów przygotowanych przez administratorów systemu informatycznego (w przypadku systemów Linux). Jako nośniki kopii zapasowych wykorzystywane są taśmy magnetyczne typu DAT/LTO zmieniane automatycznie lub ręcznie w zależności od platformy sprzętowej. Podstawowy system wykonywania kopii zarządzany

jest przez dedykowany serwer kopii zapasowych, udostępniający przestrzeń dyskową oraz automatycznie zmieniane taśmy LTO.

5.2. Kopia folderów i plików z systemów serwerowych Windows, wykonywana jest bezpośrednio na taśmy zmieniane automatycznie. Kopie z systemów typu SQL wykonywane są na dysk twardy i następnie na taśmy zmieniane automatycznie.

5.3. Kopie folderów, plików i baz danych programów uruchomionych na systemach Linux wykonywane są na dysk lokalny jako skompresowane archiwum, następnie pobierane na serwer kopii zapasowych i zapisywane na taśmach zmienianych automatycznie.

5.4. Taśmy magnetyczne typu DAT/LTO są zaewidencjonowane w „Rejestrze nośników komputerowych zawierających dane osobowe", którego wzór stanowi Załącznik Nr 6 do niniejszej Instrukcji.

5.5. Wykonywanie kopii zapasowej narzędzi programowych służących do przetwarzania danych zebranych w zbiorach nie jest wymagane. Wyjątek stanowią foldery programów, w których zapisywane są dodatkowe pliki stanowiące integralną część danych zapisanych w zbiorach (np. załączniki plikowe do treści dostępnej za pomocą przeglądarki WWW).

5.6. Szczegółowe procedury wykonywania kopii zapasowych dla poszczególnych systemów zawarte są w Załączniku Nr 7 do Instrukcji.

6. Sposób i miejsce przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych.

6.1. Należy ograniczać do minimum ilość nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane, zniszczone lub zmienione w taki sposób, aby nie było możliwe zidentyfikowanie osób, których dane dotyczyły.

6.2. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w „Polityce Bezpieczeństwa Ochrony Danych Osobowych" z wyjątkiem sytuacji wystąpienia czynników mogących uszkodzić lub zniszczyć nośniki pozostawione w obszarze przetwarzania (np. zagrożenie pożarowe). Wyniesione nośniki muszą pozostać pod kontrolą osoby, która je wyniosła, przez cały czas występowania zagrożenia lub do momentu przekazania ABI, ADO lub ASI.

6.3. Nośniki danych i kopii zapasowych (eksploatowanych dysków twardych i zmienianych automatycznie taśm magnetycznych) zawierające dane osobowe, powinny być przechowywane w urządzeniach lub, w przypadku nośników wymiennych lub uszkodzonych, w zamkniętych szafach zlokalizowanych w obszarze przetwarzania.

6.4. Elektroniczne nośniki danych wycofywane z eksploatacji należy pozbawić zapisanych treści w taki sposób, aby nie było możliwe ich odtworzenie.

6.5. W przypadku uszkodzenia elektronicznego nośnika danych zwierającego dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych lub przekazać firmie zajmującej się utylizacją tego typu urządzeń. Z wykonanych czynności należy sporządzić protokół opisujący proces zniszczenia lub przekazania do utylizacji.

6.6. Użytkownicy wykonujący samodzielnie kopię danych na nośniki wymienne odpowiedzialni są za ich bezpieczeństwo.

6.7. W przypadku przekazywania zbioru danych osobowych zapisanych na nośnikach elektronicznych podmiotom zewnętrznym, zaleca się stosowanie następujących zasad bezpieczeństwa:

1) Należy zabezpieczyć ten zbiór przed przejęciem przez osobę nieuprawnioną, za pomocą co najmniej pliku skompresowanego zabezpieczonego hasłem,
2) Hasło nie może być zapisane na nośniku elektronicznym i może być znane tylko osobie wykonującej zabezpieczenie, osobie odbierającej zbiór oraz ABI, przy czym hasło powinno być podane adresatowi inną drogą,
3) Adresat powinien zostać powiadomiony o przesyłce,
4) Należy stosować bezpieczne koperty depozytowe,
5) Przesyłkę należy przekazać osobiście do rąk osoby odbierającej lub przesłać za pośrednictwem firmy kurierskiej.

7. Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

7.1. Systemy informatyczne służące do przetwarzania danych osobowych w Uczelni narażone są na następujące grupy zagrożeń:

1) wirusy i inne złośliwe oprogramowanie rozprzestrzeniające się za pomocą nośników wymiennych, przede wszystkim pamięci typu FLASH/pendrive.
2) wirusy i inne złośliwe oprogramowanie rozprzestrzeniające się za pomocą usług internetowych typu poczta elektroniczna, oraz zainfekowane witryny internetowe, systemy wymiany plików i inne.
3) roboty internetowe i inne oprogramowanie skanujące interfejsy systemów informatycznych dostępnych z sieci publicznej Internet.
4) możliwość przechwycenia przez osoby nieuprawnione danych przesyłanych w sieciach publicznych między użytkownikami i interfejsami systemów informatycznych dostępnych w sieci publicznej Internet.

7.2. Do ochrony przed działalnością oprogramowania rozprzestrzeniającego się za pomocą nośników wymiennych stosowane jest oprogramowanie antywirusowe pracujące rezydentnie na stacjach roboczych. W celu minimalizacji ewentualnych infekcji, użytkownicy nie mają praw administracyjnych do systemów operacyjnych komputerów zainstalowanych w obszarze

przetwarzania. Zabronione jest samowolne podłączanie przez użytkowników komputerów, nośników używanych w urządzeniach pozostających poza kontrolą Uczelnianych administratorów systemów informatycznych. W uzasadnionych przypadkach, dostarczony nośnik powinien zostać przed podłączeniem sprawdzony przez ASI w celu eliminacji ewentualnego zagrożenia. Zabronione jest ładowanie telefonów komórkowych i innych urządzeń z portów USB komputerów służących do przetwarzania danych osobowych.

7.3. Do ochrony przed działalnością oprogramowania rozprzestrzeniającego się za pomocą usług internetowych stosuje się oprogramowanie antywirusowe z funkcjonalnością skanowania poczty elektronicznej oraz lokalną zaporę sieciową wbudowaną w oprogramowanie antywirusowe lub system operacyjny. Dodatkowo ograniczana jest dostępność usług sieci publicznej Internet za pomocą dedykowanego urządzenia typu Firewall posiadającego funkcjonalność filtra antyspamowego oraz możliwość skanowania antywirusowego.

7.4. Do ochrony systemów informatycznych dostępnych z sieci publicznej przed robotami internetowymi i innymi zagrożeniami, stosuje się dedykowane urządzenie typu zapora Firewall w celu ograniczenia możliwości inicjalizacji ruchu z sieci publicznej, tylko do określonych usług oraz lokalne mechanizmy filtrowania, wbudowane w systemy operacyjne udostępniające usługi w sieci publicznej.

7.5. Do ochrony przed przechwyceniem danych przesyłanych w sieciach publicznych stosuje się metody kryptograficznej ochrony danych za pomocą technologii takich jak SSL, VPN. Zabronione jest udostępnianie możliwość inicjowania komunikacji z sieci publicznych z usługami nie obsługującymi technologii ochrony kryptograficznej.

8. Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

8.1. Dane osobowe udostępnia się odbiorcy danych na pisemny wniosek ze wskazaniem przez odbiorcę podstawy prawnej legalizującej przetwarzanie danych osobowych (art. 23 lub art. 27 ustawy o ochronie danych osobowych).

8.2. Zgody na udostępnienie danych udziela ABI, który odpowiada również za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem.

8.3. ABI odnotowuje zdarzenia udostępnienia w rejestrze odbiorców danych osobowych. W rejestrze odnotowywane są między innymi: imię i nazwisko lub nazwa odbiorcy, adres odbiorcy, podstawa prawna udostępnienia, data udostępnienia oraz zakres udostępnienia. Dopuszcza się załączanie do rejestru wydruku/kopii papierowej przekazanego zbioru danych. Wzór rejestru odbiorców danych osobowych stanowi Załącznik Nr 8 do Instrukcji.

8.4. W sytuacji kiedy system informatyczny umożliwia odnotowywanie informacji o odbiorcach danych, możliwe jest prowadzenie rejestru elektronicznego.

8.5. Na żądanie osoby, której dane zostały udostępnione odbiorcy danych, ABI udostępnia właściwe informacje na podstawie prowadzonego rejestru lub wygenerowanego raportu w systemie informatycznym, jeśli program udostępnia funkcjonalność rejestracji odbiorców danych.

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

9.1. Za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty e-mail, a także za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.

9.2. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych nadzorowane są przez Administratora Bezpieczeństwa Informacji i wykonywane są przez administratorów właściwych systemów informatycznych w pomieszczeniach stanowiących obszar przetwarzania danych.

9.3. Przeglądy techniczne i konserwacja systemu powinny być wykonywane w terminach określonych przez producentów lub zgodnie z harmonogramem ASI, jednak nie rzadziej niż raz w roku, a także w trakcie przygotowania do dużych aktualizacji systemów.

9.4. Przeglądy i konserwacje w zależności od systemu, powinny zawierać czynności związane z:

1) analizą zdarzeń i logów systemowych w celu wykrycia niestandardowych zachowań,
2) kontrolą zajętości dysku twardego oraz usuwanie zbędnych danych (np. bardzo stare logi zdarzeń, pliki tymczasowe „temp", tymczasowe kopie zbiorów danych, itp.)
3) kontrolą obciążenia procesora i uruchomionych procesów w systemie operacyjnym,
4) kontrolą poprawności funkcjonowania zabezpieczeń przed nieuprawnionym dostępem do zbiorów.

9.5. W przypadku konieczności naprawy sprzętu przez podmiot zewnętrzny, należy:

1) zawrzeć umowę na wykonywanie czynności serwisowych, zawierającą zobowiązanie podmiotu zewnętrznego do zachowania w tajemnicy informacji, które mogą znajdować się na wbudowanym nośniku przechowującym dane,
2) przed jego przekazaniem do naprawy należy wymontować nośniki danych lub usunąć dane w sposób uniemożliwiający ich odtworzenie,
3) zlecić naprawę w obecności ASI lub osoby przez niego upoważnionej, gdy nie ma możliwości usunięcia danych z nośnika.

9.6. Zabronione jest samowolne wykonywanie lub zlecanie podmiotom zewnętrznym napraw, przeglądów i konserwacji sprzętu komputerowego służącego do przetwarzania danych osobowych, przez osoby nie będące pracownikami Działu Systemów Komputerowych PWSIiP w Łomży.

9.7. Naprawy, przeglądy i konserwacje należy odnotowywać w dzienniku eksploatacji systemu informatycznego, którego wzór stanowi Załącznik Nr 9 do Instrukcji.

10. Procedura dostępu podmiotów zewnętrznych

10.1. Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa Administrator Danych.

10.2. Z podmiotami zewnętrznymi (np. firma wdrażająca oprogramowanie komputerowe, firma ochroniarska), które mają dostęp do danych osobowych na terenie Uczelni, należy zawrzeć umowę zawierającą zapisy o powierzeniu zbioru danych osobowych do przetwarzania wraz z klauzulą poufności.

10.3. Podmiot zewnętrzny zobowiązany jest do zachowania poufności powierzonych danych i przetwarzania ich zgodnie z celem umowy.

10.4. Administrator Bezpieczeństwa Informacji prowadzi rejestr podmiotów zewnętrznych, którym Administrator Danych Osobowych udzielił upoważnienia do przetwarzania danych osobowych. Wzór rejestru zawiera Załącznik Nr 10 do Instrukcji.

11 Spis załączników do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w PWSIiP w Łomży:

Załącznik nr 1 – Wzór wniosku o udzielenie/odwołanie upoważnienia do przetwarzania danych osobowych

Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 3 - Wzór odwołania upoważnienia do przetwarzania danych osobowych

Załącznik nr 4 – Wzór rejestru osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 5 – Wzór wniosku o udostępnienia hasła innemu użytkownikowi

Załącznik nr 6 – Wzór rejestru nośników komputerowych

Załącznik nr 7 – Wzór Procedur wykonywania kopii zapasowych

Załącznik nr 8 - Wzór rejestru odbiorców danych osobowych

Załącznik nr 9 – Wzór dziennika eksploatacji systemu informatycznego

Załącznik nr 10 – Wzór rejestru podmiotów zewnętrznych

REKTOR
dr hab. Robert Charmas, prof. PWSIiP