Załącznik Nr 1 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

Polityka Bezpieczeństwa Ochrony Danych Osobowych

w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży

Spis treści

1. Postanowienia ogólne 3
2. Zadania ABI ustawowe i scedowane przez ADO 5
3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe 6
4. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych 6
5. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi 7
6. Sposób przepływu danych pomiędzy poszczególnymi systemami 7
7. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych 7
8. Procedura postępowania z incydentami (Instrukcja alarmowa) 9
9. Procedura działań korygujących i zapobiegawczych 11
10. Kontrola wewnętrzna stanu ochrony danych osobowych 11
11. Zarządzanie systemem ochrony danych 12
12. Szkolenia lub zapoznawanie osób z zasadami ochrony danych osobowych 13
13. Postanowienia końcowe 14
14. Spis załączników do Polityki Bezpieczeństwa Ochrony Danych Osobowych: 15

1. Postanowienia ogólne

1.1 Polityka Bezpieczeństwa Ochrony Danych Osobowych została opracowana zgodnie z wymogami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz. 1182 z późn. zm.), oraz wymaganiami określonymi w § 4 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).

1.2 Celem Polityki Bezpieczeństwa Ochrony Danych Osobowych jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby zapewnić właściwą ochronę danych osobowych, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną oraz zapewnić ochronę prywatności osób, których dane są przetwarzane.

Opisane i zastosowane w niej zabezpieczenia mają zapewnić:

1) poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały w sposób nieautoryzowany zmienione lub zniszczone,
3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

1.3. Przez użyte w Polityce Bezpieczeństwa Ochrony Danych Osobowych określenia, należy rozumieć:

1) Administrator Danych Osobowych, ADO – Rektor Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży, decydujący o celach i środkach przetwarzania danych osobowych;
2) Administrator Bezpieczeństwa Informacji, ABI – osoba powołana przez ADO, odpowiedzialna za organizację ochrony danych osobowych;
3) Ustawa – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 r. poz. 1182 z późn. zm.);
4) Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów;
6) Usuwanie danych – zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

7) Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie, zmienianie i usuwanie;
8) System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
9) Administrator Systemu Informatycznego, ASI - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
10) Użytkownik – osoba posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
11) Zabezpieczenie systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnioną modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,
12) Nośnik komputerowy – nośnik służący do zapisu i przechowywania informacji, np. pendrive, płyty CD/DVD, dyski twarde;
13) Kierownik komórki organizacyjnej – należy przez to rozumieć kierowników jednostek i komórek organizacyjnych, w których zatrudnieni są pracownicy przetwarzający dane osobowe;
14) PWSIiP, Uczelnia – Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży;
15) GIODO – Generalny Inspektor Ochrony Danych Osobowych;
16) Incydent - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
17) Zagrożenie – potencjalna możliwość wystąpienia incydentu;
18) Działanie korygujące – jest to działanie przeprowadzane w celu wyeliminowania przyczyny i skutku incydentu lub innej niepożądanej sytuacji;
19) Działanie zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej;
20) Kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, Polityki Bezpieczeństwa Ochrony Danych Osobowych i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

1.4. Zestaw dokumentów Polityki Bezpieczeństwa Ochrony Danych Osobowych składa się z:

1) niniejszego dokumentu Polityki Bezpieczeństwa Ochrony Danych Osobowych w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży, dalej zwanego Polityką Bezpieczeństwa, wraz z załącznikami,
2) Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych

osobowych w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży, dalej zwaną Instrukcją Zarządzania, wraz z załącznikami.

1.5. Zakresy określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do całego systemu informacyjnego Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży, w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz zbiorów papierowych, w których przetwarzane są informacje podlegające ochronie,
2) informacji będących własnością Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży lub jej kontrahentów, o ile zostały przekazane na podstawie umów,
3) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

2. Zadania ABI ustawowe i scedowane przez ADO

2.1. Do ustawowych obowiązków ABI należy:

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO,
2) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 ustawy o ochronie danych osobowych, oraz przestrzegania zasad w niej określonych,
3) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
4) prowadzenie rejestru zbiorów danych przetwarzanych przez ADO, z wyjątkiem zbiorów zawierających dane wrażliwe.

2.2. Do pozostałych obowiązków ABI scedowanych przez ADO należy:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa ,
3) wydawanie i odwoływanie upoważnień do przetwarzania danych osobowych,
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6) nadzór nad bezpieczeństwem danych osobowych,
7) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

2.3. Administrator Bezpieczeństwa Informacji ma prawo :

1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji,
2) wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych, w celu oceny zgodności przetwarzania danych z przepisami prawa,
3) żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4) żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5) żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

3.1 Obszar, w którym przetwarzane są dane osobowe stanowią budynki, w których Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży realizuje swoje zadania statutowe.

3.2 Szczegółowe rozmieszczenie zbiorów w postaci dokumentacji papierowej i elektronicznej, zawierających dane osobowe, opisane jest w Wykazie budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych, którego wzór stanowi Załącznik Nr 1.

3.3. Administrator budynku zobowiązany jest przekazać ABI niezwłocznie, nie później jednak niż w terminie 7 dni, informację o zmianach w przeznaczeniu pomieszczeń.

4. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

4.1. Dane osobowe w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży przetwarzane są w celu realizacji statutowych celów szkoły wyższej. W szczególności dane osobowe przetwarza się:

1) dla zabezpieczenia prawidłowego toku realizacji zadań dydaktycznych, naukowych i organizacyjnych Uczelni, wynikających z przepisów ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (tekst jedn. Dz. U. z 2012 r, poz. 572 z późn. zm.),
2) w celu zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni polityki personalnej oraz bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia, nawiązywanych przez Uczelnię, działającą jako pracodawca w rozumieniu art. 3 Kodeksu pracy lub strona innych stosunków zatrudnienia,
3) dla realizacji innych usprawiedliwionych celów i zadań PWSIiP w Łomży, z poszanowaniem praw i wolności osób powierzających Uczelni swoje dane.

4.2. Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej opisany jest w Wykazie zbiorów danych osobowych, którego wzór stanowi Załącznik Nr 2.

4.3. Wykaz programów stosowanych do przetwarzania danych osobowych zawartych w w/w zbiorach zawarty jest w Wykazie programów zastosowanych do przetwarzania danych osobowych, którego wzór stanowi Załącznik Nr 3.

5. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

5.1. Dane osobowe przetwarzane w systemach informatycznych PWSIiP w Łomży zapisywane są w systemach zarządzania relacyjnych baz danych typu SQL. Mogą też być zapisywane w postaci plików arkuszy kalkulacyjnych i baz danych typu MS Access.

5.2. Opis struktury zbiorów danych osobowych przedstawiono w Załącznikach nr 4 Opis pól informacyjnych i powiązań między nimi lub przedstawiających widoki formularzy.

6. Sposób przepływu danych pomiędzy poszczególnymi systemami

6.1. Przetwarzanie danych osobowych w PWSIiP w Łomży odbywa się z wykorzystaniem systemów informatycznych wykonanych w różnych technologiach, przechowujących informacje w różnych systemach zarządzania bazą danych. W celu ograniczenia ilości pracy związanej wprowadzaniem danych oraz z eliminacją błędów, które mogą być popełniane przez użytkowników, stosuje się techniki integracji systemów informatycznych, zapewniające przepływ danych między systemami. Przepływ danych pomiędzy poszczególnymi systemami może odbywać się za pomocą plików tekstowych, komunikacji bezpośredniej z wykorzystaniem interfejsów SQL lub komunikacji pośredniej z wykorzystaniem interfejsów typu API.

6.2. Sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe przedstawiono w załączniku pod nazwą Sposób przepływu danych, którego wzór stanowi Załącznik Nr 5.

6.3. Przetwarzanie danych osobowych w PWSIiP w Łomży realizowane jest w różnych systemach informatycznych, dostępnych również poza podstawowym obszarem przetwarzania danych. W związku z dostępnością niektórych systemów z sieci publicznej stosuje się wysoki poziom zabezpieczenia systemów informatycznych służących do przetwarzania danych osobowych.

7. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

7.1 Zabezpieczenia organizacyjne:

1) Został wyznaczony Administrator Bezpieczeństwa Informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych.
2) Została opracowana i wdrożona Polityka Bezpieczeństwa.

3) Została opracowana i wdrożona Instrukcja Zarządzania Systemem Informatycznym.
4) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez ABI.
5) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
6) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz rozwiązaniami w zakresie zabezpieczeń systemu informatycznego.
7) Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.
8) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
9) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko za zgodą ABI lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzór upoważnienia do przebywania w obszarze przetwarzania danych stanowi Załącznik Nr 6. Z wnioskiem o udzielenie upoważnienia występują kierownicy jednostek zatrudniających pracownika lub zlecających prace.
10) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.

7.2 Zabezpieczenia fizyczne pomieszczeń z danymi osobowymi w wersji papierowej i elektronicznej:

1) Zabezpieczenia fizyczne opisane są w sposób szczegółowy w Załączniku Nr 1 Wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych w PWSIiP w Łomży.
2) Klucze do pomieszczeń pobierane są z portierni. Pobranie i zwrot klucza odnotowywane jest w książce pobrań lub rejestrowane elektronicznie w programie SYSTEM_KLUCZY.

7.3 Zabezpieczenie dokumentów i wydruków

1) Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
2) Pracownicy są zobowiązani do zabezpieczania dokumentów (np. zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy - tzw. polityka czystego biurka.
3) Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.
4) Niszczenie dokumentów zawierających dane osobowe, w tym wydruków tymczasowych musi odbywać się z użyciem niszczarek.
5) Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy komórek organizacyjnych oraz podległe im osoby przetwarzające dane osobowe.

7.4 Zabezpieczenia infrastruktury informatycznej

7.4.1. W celu ochrony danych osobowych przetwarzanych w PWSIiP w Łomży stosuje się następujące metody:

1) Konta użytkowników zabezpieczone hasłem.
2) Dostęp do komputerów zainstalowanych w obszarze przetwarzania danych możliwy jest po zalogowaniu do systemu operacyjnego.
3) Użytkownicy komputerów zainstalowanych w obszarze przetwarzania danych posiadają ograniczone uprawnienia do zasobów systemu operacyjnego.
4) Na komputerach zainstalowanych w obszarze przetwarzania danych uruchomione jest oprogramowanie antywirusowe.
5) Komunikacja między siecią lokalną, a siecią publiczną jest separowana za pomocą urządzeń typu Firewall z funkcjonalnościami filtrowania antyspamowego i antywirusowego.
6) Możliwość wglądu w pełny zestaw danych osobowych oraz ich modyfikacji ograniczono tylko do komputerów zainstalowanych w pomieszczeniach stanowiących obszar przetwarzania danych.
7) W systemach dostępnych z sieci publicznej istnieje jedynie możliwość wglądu w podstawowe dane identyfikacyjne typu imię, nazwisko, nr indeksu, nr telefonu, adres e-mail, w celach komunikacyjnych oraz przypisywania innych informacji np. wysyłanie wiadomości tekstowych, wpisywanie ocen, przydzielanie zadań, materiałów dydaktycznych i testów.
8) Stosuje się zabezpieczenia kryptograficzne aplikacji dostępnych z sieci publicznej.
9) Ogranicza się do niezbędnego minimum ilość interfejsów, do których można inicjować komunikację z sieci publicznej.
10) W uzasadnionych sytuacjach możliwy jest zdalny dostęp do zasobów w obszarze przetwarzania danych za pomocą szyfrowanych połączeń VPN z użyciem technik pulpitu zdalnego, w celu wyeliminowania przesyłania danych na komputer znajdujący się poza obszarem przetwarzania danych. Dostęp zdalny realizowany jest na podstawie „Regulaminu Sieci Komputerowej PWSIiP w Łomży".
11) Wykonywane są regularnie kopie zapasowe zbiorów zawierających dane osobowe.

7.4.2. Szczegółowe informacje na temat zarządzania systemem informatycznym oraz określenie zabezpieczeń zawarte są w pkt. 7 Instrukcji Zarządzania.

8. Procedura postępowania z incydentami (Instrukcja alarmowa)

8.1. Procedura definiuje katalog zdarzeń zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów zagrażających bezpieczeństwu oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

8.2. Każda osoba upoważniona do przetwarzania danych osobowych oraz zobowiązana do zachowania poufności danych osobowych, w przypadku stwierdzenia zagrożenia lub

naruszenia ochrony danych osobowych, zobowiązana jest poinformować o tym fakcie bezpośredniego przełożonego lub Administratora Bezpieczeństwa Informacji. Wzór zgłoszenia zawiera Załącznik Nr 7 Meldunek o naruszeniu bezpieczeństwa.

8.3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka oraz czystego ekranu, zasad ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

8.4. Do typowych incydentów naruszenia bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

8.5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające, w toku którego:

1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
2) inicjuje ewentualne działania dyscyplinarne,
3) rekomenduje działania prewencyjne zmierzające do eliminacji podobnych zagrożeń w przyszłości,
4) dokumentuje prowadzone postępowania.

8.6. W przypadku stwierdzenia incydentu (naruszenia), Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające, w toku którego:

1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
2) zabezpiecza ewentualne dowody,
3) ustala osoby odpowiedzialne za naruszenie,
4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
5) inicjuje działania dyscyplinarne,
6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
7) dokumentuje prowadzone postępowania.

9. Procedura działań korygujących i zapobiegawczych

9.1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów naruszających bezpieczeństwo lub powodujących zagrożenia systemu ochrony danych osobowych.

9.2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie procesy, w których incydenty naruszające bezpieczeństwo lub powodujące zagrożenia mogą wpłynąć na zgodność z wymaganiami ustawy o ochronie danych osobowych, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.

9.3. Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji.

9.4. Opis czynności:

1) ABI jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
   a) zgłoszenia od pracowników,
   b) wiedza ABI,
   c) wyniki kontroli wewnętrznych związanych z ochroną danych osobowych, kontroli GIODO lub pozostałych.
2) W przypadku, gdy ABI stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną.
3) ABI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4) Po przeprowadzeniu działań korygujących lub zapobiegawczych, ABI jest zobowiązany do oceny efektywności ich zastosowania.

9.5. Powyższe czynności ABI rejestruje w dzienniku, którego wzór stanowi Załącznik Nr 8 Rejestr incydentów bezpieczeństwa, działań korygujących i zapobiegawczych.

10. Kontrola wewnętrzna stanu ochrony danych osobowych

10.1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych ze sprawdzaniem zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.

10.2. Do kontroli stanu ochrony danych osobowych upoważniony jest ABI.

10.3. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami ustawy o ochronie danych osobowych.

10.4. ABI przygotowuje plan kontroli uwzględniając cel, zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.

10.5. ABI jest ustawowo zobligowany do wykonania kontroli na zlecenie GIODO. Sprawozdanie po tej kontroli jest przedkładane do ADO oraz do GIODO.

10.6. Kontrola przeprowadzana jest na podstawie listy stanowiącej Załącznik Nr 9 Lista kontrolna ochrony danych osobowych.

10.7. ABI może dokumentować przebieg kontroli w postaci danych i wydruków z kontrolowanych systemów (programów) oraz poprzez sporządzanie: notatek z czynności, protokołów odebrania ustnych wyjaśnień, protokołów z oględzin, kopii dokumentów, printscreenów, logów systemowych, zapisów konfiguracji technicznych środków zabezpieczeń systemów.

10.8. Po dokonanej kontroli ABI przygotowuje i przekazuje ADO raport pokontrolny, którego wzór stanowi Załącznik Nr 10 Sprawozdanie pokontrolne. Na jego podstawie inicjowane są działania korygujące lub zapobiegawcze.

11. Zarządzanie systemem ochrony danych

11.1. Procedura przeglądu i aktualizacji Polityki Bezpieczeństwa wraz z Instrukcją Zarządzania

1) ABI odpowiada za weryfikację dokumentacji, aby Polityka Bezpieczeństwa i Instrukcja Zarządzania były: opracowane, kompletne, aktualne oraz zgodne z przepisami prawa,
2) ABI odpowiada za weryfikację skuteczności zabezpieczeń techniczno-organizacyjnych opisanych w Polityce Bezpieczeństwa i Instrukcji Zarządzania,
3) ABI odpowiada za weryfikację przestrzegania obowiązków nałożonych na osoby opisane w Polityce Bezpieczeństwa i Instrukcji Zarządzania,
4) w przypadku wykrycia podczas weryfikacji nieprawidłowości, ABI zawiadamia ADO o nieopracowaniu lub brakach w dokumentacji oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu prawnego (np. aktualizacja dokumentacji, instruowanie osób o prawidłowych procedurach działania, wnioski o sankcje dla osób naruszających zasady ochrony danych osobowych).

11.2. Zarządzanie wewnętrznym rejestrem zbiorów

1) prowadzenie rejestru jest wyłączną rolą ABI; wzór rejestru stanowi Załącznik Nr 11;
2) w stosunku do każdego zbioru danych w rejestrze dokumentowane są podstawowe informacje o zbiorze, w tym nazwa zbioru, oznaczenie Administratora Danych Osobowych prowadzącego zbiór, cel, zakres, podstawa prawna przetwarzania,

kategorie osób, których dane są przetwarzane w zbiorze, sposób zbierania i udostępniania danych,

3) ABI jest zobowiązany do wpisu w rejestrze nowego zbioru, odnotowania zmiany informacji przetwarzanych w zbiorze oraz odnotowania faktu zaprzestania przetwarzania danych w zbiorze. Osoby zamierzające utworzyć nowy zbiór danych osobowych obowiązane są przekazać ABI informacje dotyczące zbioru. ABI lub ADO może zakazać przetwarzania danych w nie zgłoszonym do rejestru zbiorze,
4) rejestr zbiorów może być prowadzony w formie papierowej lub elektronicznej. Kopia części jawnej rejestru udostępniana jest na stronie internetowej Uczelni w postaci dokumentu elektronicznego, który po każdej modyfikacji rejestru powinien być aktualizowany,
5) w przypadku prowadzenia rejestru w postaci papierowej, ABI udostępnia każdemu zainteresowanemu jego treść w siedzibie ADO.

11.3. ABI może organizować roczne spotkanie podsumowujące stan ochrony danych osobowych, na którym dokonywana jest ocena funkcjonowania systemu ochrony danych osobowych oraz planowane są działania związane z poprawą stanu ochrony danych osobowych. Uczestnikami spotkania są: ABI oraz wybrane osoby odpowiedzialne za stan ochrony danych osobowych w Uczelni. Raport ze spotkania przygotowany jest według wzoru z Załącznika Nr 12 Sprawozdanie dotyczące ochrony danych osobowych i przedkładany ADO.

12. Szkolenia lub zapoznawanie osób z zasadami ochrony danych osobowych

12.1. Każda osoba przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami w wersji papierowej, winna być poddana przeszkoleniu lub zapoznana z przepisami dotyczącymi ochrony danych osobowych wraz z zasadami ochrony danych osobowych ujętymi w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania.

12.2. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych zdarzenie powyższe dokumentuje się za pomocą Planu szkolenia, którego wzór stanowi Załącznik Nr 13.

12.3. Każda osoba po szkoleniu lub po zapoznaniu z zasadami ochrony danych osobowych zobowiązana jest do podpisania oświadczenia o poufności, którego wzór stanowi Załącznik Nr 14 Oświadczenie o poufności.

12.4. Podpisane Oświadczenia o poufności są przechowywane w aktach osobowych pracowników, a kopie w dokumentacji ABI.

12.5. Podpisane Oświadczenia o poufności stanowią podstawę do nadania upoważnienia do przetwarzania danych osobowych.

13. Postanowienia końcowe

13.1. Polityka Bezpieczeństwa wraz z załącznikami jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody ADO.

13.2. Polityka Bezpieczeństwa może być udostępniania osobom i instytucjom postronnym bez zgody ADO, jeżeli nie zawiera w treści informacji o zabezpieczeniach danych osobowych, a wszelkie załączniki występują w formie niewypełnionych szablonów.

13.3. Osoby przetwarzające dane osobowe, zarówno pracownicy w rozumieniu Kodeksu Pracy, jak i osoby świadczące pracę na podstawie umów cywilnoprawnych, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie, zobowiązane są do stosowania postanowień zawartych w niniejszej Polityce Bezpieczeństwa.

13.4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

13.5. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. 2014 r. poz. 1182 z późn. zm.), oraz wydanych na jej podstawie aktów wykonawczych.

14. Spis załączników do Polityki Bezpieczeństwa Ochrony Danych Osobowych:

1. Załącznik Nr 1 – wzór Wykazu budynków i pomieszczeń
2. Załącznik Nr 2 - wzór Wykazu zbiorów danych osobowych
3. Załącznik Nr 3 - wzór Wykazu programów do przetwarzania danych osobowych
4. Załączniki Nr 4 – Opis pól informacyjnych i powiązań między nimi lub przedstawiających widoki formularzy (do użytku wewnętrznego)
5. Załącznik Nr 5 - Sposób przepływu danych (wzór)
6. Załącznik Nr 6 – wzór Upoważnienia do przebywania w obszarze przetwarzania danych
7. Załącznik Nr 7 – wzór Meldunku o naruszeniu bezpieczeństwa
8. Załącznik Nr 8 – wzór Rejestru incydentów bezpieczeństwa i działań korygujących i zapobiegawczych
9. Załącznik Nr 9 – Lista kontrolna
10. Załącznik Nr 10 – wzór Sprawozdania pokontrolnego
11. Załącznik Nr 11 - wzór Rejestru zbiorów danych osobowych
12. Załącznik Nr 12 – wzór Sprawozdania dotyczącego ochrony danych osobowych
13. Załącznik Nr 13 – Plan szkolenia
14. Załącznik Nr 14 – wzór Oświadczenia o poufności

REKTOR
dr hab. Robert Charmas, prof. PWSIiP