Zarządzenie nr 3
Rektora Uniwersytetu w Białymstoku
z dnia 14 marca 2012 r.

w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych Uniwersytetu w Białymstoku

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (T.J. z roku 2002 Dz. U. Nr 101 poz. 926 z późn. zm.) w związku z Rozporządzeniem 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) zarządza się co następuje:

§ 1

Wprowadza się *Politykę bezpieczeństwa danych osobowych Uniwersytetu w Białymstoku*, stanowiącą Załącznik do niniejszego Zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR
UNIWERSYTETU w BIAŁYMSTOKU
prof. dr hab. Jerzy Nikitorowicz

Załącznik
do Zarządzenia nr 3
Rektora Uniwersytetu w Białymstoku
z dnia 14 marca 2012 r.

Polityka bezpieczeństwa danych osobowych Uniwersytetu w Białymstoku

1. Wstęp

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych, przetwarzanych przez Uniwersytet w Białymstoku.

Polityka została opracowana zgodnie z wymogami 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).

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje, oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i 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 zmienione lub zniszczone w sposób nieautoryzowany,
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.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj.Dz. U z 2002r. Nr 101, poz. 926 z późn. zm.),
2. oraz aktami wykonawczymi wydanymi na podstawie wskazanej wyżej ustawy.

2. Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka – Polityka bezpieczeństwa danych osobowych w Uniwersytecie w Białymstoku.
2. Administrator Danych Osobowych – Uniwersytet w Białymstoku, decydujący o celach i środkach przetwarzania danych osobowych;
3. Administrator Bezpieczeństwa Informacji (ABI) – pracownik Uniwersytetu w Białymstoku, wyznaczony przez Rektora Uniwersytetu w Białymstoku, odpowiedzialny za organizację ochrony danych osobowych.
4. Ustawa – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r.Nr 101, poz.926 z późn. zm.)
5. Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;
7. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
8. Zgoda osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
9. Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych w pamięci (również zewnętrznej) komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
10. Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, przechowywanie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
11. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
12. Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
13. Użytkownik - pracownik Uniwersytetu w Białymstoku posiadający uprawnienia do pracy w systemie informatycznym, zgodnie z zakresem obowiązków służbowych;
14. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych, oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,
15. Nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, pamięci USB (pendrive), karty pamięci;

3. Zadania Administratora Bezpieczeństwa Informacji (ABI)

Do najważniejszych obowiązków Administratora Bezpieczeństwa Informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki,
3. wydawanie i anulowanie upoważnień do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład dla osób przetwarzających dane osobowe,
4. prowadzenie „Rejestru osób zatrudnionych przy przetwarzaniu danych osobowych",
5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia bezpieczeństwa 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.

Administrator Bezpieczeństwa Informacji ma prawo:

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Uniwersytecie w Białymstoku,
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 ustawą,
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,

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

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, jest sporządzany i aktualizowany przez ABI zgodnie z wzorem stanowiącym Załącznik A do niniejszej Polityki.

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

Opis struktury zbiorów danych osobowych przedstawiony został w Załączniku B do niniejszej Polityki.

6. Sposób przepływu danych pomiędzy poszczególnymi systemami

Sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe przedstawiony został w Załączniku C do niniejszej Polityki.

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

A) Zabezpieczenia organizacyjne:

1. Wyznaczenie administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych.
2. Opracowanie i wdrożenie polityki bezpieczeństwa.
3. Opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym.
4. Dopuszczanie do przetwarzania danych wyłącznie osób posiadających upoważnienia nadane przez administratora danych.
5. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych.
6. Przeszkolenie osób zatrudnionych przy przetwarzaniu danych w zakresie przepisów dotyczących ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego.
7. Zobowiązanie osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania ich w tajemnicy.
8. Przetwarzanie danych osobowych wyłącznie w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
9. Dopuszczenie do przebywania osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych, z zachowaniem warunków zapewniających bezpieczeństwo danych.

10. Przetwarzanie danych, których administratorem jest Uniwersytet w Białymstoku, może być powierzone podmiotom zewnętrznym wyłącznie na podstawie umowy w formie pisemnej, której treść zapewnia przestrzeganie polityki bezpieczeństwa.

B) Zabezpieczenia ochrony fizycznej danych osobowych.
Katalog zabezpieczeń fizycznych wskazano w Załączniku A.

C) Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej.
Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

D) Zabezpieczenia narzędzi programowych i baz danych.
Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

8. Instrukcja alarmowa

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest ograniczenie ryzyka powstania zagrożeń oraz minimalizacja skutków wystąpienia zagrożeń.

1. Każdy pracownik Uniwersytetu w Białymstoku w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub Administratora Bezpieczeństwa Informacji.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
3. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
    c. 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).
4. W przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające, w toku którego:
    a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
    b. inicjuje ewentualne działania dyscyplinarne,
    c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

d. dokumentuje czynności podjęte w prowadzonym postępowaniu.

5. W przypadku stwierdzenia naruszenia bezpieczeństwa danych, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające, w toku którego:
   a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   b. zabezpiecza ewentualne dowody,
   c. ustala osoby odpowiedzialne za naruszenie,
   d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   e. inicjuje działania dyscyplinarne,
   f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   g. dokumentuje czynności podjęte w prowadzonym postępowaniu.

9. Procedura działań korygujących i zapobiegawczych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych, wynikających z zaistnienia naruszeń lub zagrożeń bezpieczeństwa danych, oraz zagrożeń systemu ochrony danych osobowych.
2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami ustawy o ochronie danych osobowych, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji.

Definicje

1. Incydent - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
2. Zagrożenie – potencjalna możliwość wystąpienia incydentu.
3. Korekcja – działanie w celu wyeliminowania skutków incydentu.
4. Działanie korygujące – jest to działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji.
5. Działanie zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.
6. Kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki i instrukcji.

Opis czynności

1. ABI jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
   - zgłoszenia od pracowników,
   - wiedza ABI,
   - wyniki kontroli,
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.
5. Powyższe czynności ABI odnotowuje w Rejestrze bezpieczeństwa i działań korygujących i zapobiegawczych, którego wzór stanowi Załącznik D.

10. Kontrola systemu ochrony danych osobowych

1. Celem kontroli jest weryfikacja przestrzegania polityki i stanu bezpieczeństwa danych osobowych.
2. Kontrola obejmuje wszystkie prowadzone w Uniwersytecie działania, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
3. Do kontroli stanu ochrony danych osobowych upoważniony jest Rektor UwB, ABI, wyznaczeni kontrolerzy wewnętrzni,
4. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami U.O.D.O.
5. Administrator Bezpieczeństwa Informacji przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.
6. Po dokonanej kontroli przeprowadzający kontrolę przygotowuje i przekazuje raport pokontrolny sporządzony zgodnie z wzorem, stanowiącym Załącznik E do niniejszej Polityki, kierownikowi kontrolowanej jednostki lub komórki organizacyjnej oraz Administratorowi Danych Osobowych. Na jego podstawie ABI inicjuje działania korygujące lub zapobiegawcze.

11. Sprawozdanie roczne stanu systemu ochrony danych osobowych

1. Raz w roku Administrator Bezpieczeństwa Informacji przygotowuje sprawozdanie roczne ze stanu funkcjonowania systemu ochrony danych osobowych.
2. W spotkaniu sprawozdawczym uczestniczą: ABI, Kierownicy działów, w których przetwarzane są dane osobowe, Informatyk.
3. Raport, przygotowany zgodnie z wzorem stanowiącym Załącznik F do niniejszej Polityki, przedstawiany jest Rektorowi.

12. Szkolenia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada ABI a za jego zorganizowanie odpowiada przełożony użytkowników.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami

wykonawczymi oraz instrukcjami obowiązującymi Administratora Danych. Szczegółowy zakres szkolenia ze wzorem listy obecności określa Załącznik G do niniejszej Polityki.

4. Po zakończeniu szkolenia słuchacz podpisuje Oświadczenie o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych, którego wzór stanowi Załącznik H do niniejszej Polityki. Oświadczenie przechowywane jest w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

13. Postanowienia końcowe

1. „Polityka Bezpieczeństwa" jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Kierownicy jednostek organizacyjnych obowiązani są do zapoznania z treścią Polityki każdego użytkownika korzystającego z systemu przetwarzającego dane osobowe.
3. Wszystkie zasady dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce".
5. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
6. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
7. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
8. W sprawach nieuregulowanych w niniejszej „Polityce bezpieczeństwa" mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tj. Dz.U. z 2002r., Nr 101, poz. 926 ze zm.) oraz wydanych na jej podstawie aktów wykonawczych.

Załącznik A – Wykaz zbiorów danych osobowych na Uniwersytecie w Białymstoku

Legenda:

(1) nazwa zwyczajowa lub własna, np.: dane osobowe, dokumentacja ZFŚS, baza klientów stałych,

(2) np.: mySQL, Oracle, MS SQL, PostgreSQL, baza zewnętrza (outsourcing)

(3) np.; (I) indywidualne hasło dostępu do bazy danych, (S) szyfrowanie danych, (F) wydzielona fizycznie sieć, (UPSB) – UPS bazy

(4) (S) – serwerownia, (K) – miejsce przechowywania kopii bezpieczeństwa, (U) – pomieszczenia użytkowników, (PI) – pomieszczenie informatyka

(5) (K) – kraty w oknach, (A) – alarm, (W) – wzmocnienie drzwi, (D) – dozór całodobowy, (KD) – kontrola dostępu, (KL) – klimatyzacja, (SP) – sygnalizacja PPOŻ, (GAS) –gaśnice, (ZP) – zamki patentowe, (SF)- Sejf, (SO) – Sejf Ogniotrwały, (SK)- szafa zamykana na klucz, (UPS) – UPS stacji

Lp.	Nazwa zbioru danych (1)	Baza danych(2)	Zabezpieczenie Bazy (3)	Program służący do przetwarzania baz danych	Rejestracja w GIODO?	Lokalizacja	Nr pokoju	Funkcja lokalizacji (4)	Zabezpieczenia fizyczne (5)	Podstawa przetwarzania
1										
2										
3										
4										
5										
6										
7										
8										
10										

Załącznik C - Sposób przepływu danych pomiędzy poszczególnymi systemami

System (Moduł) A	System (Moduł) B	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Program kadrowo-płacowy	Program Płatnik	Jednokierunkowo z programu kadrowo – płacowego do programu Płatnik	Półautomatycznie – eksport pliku z programu kadrowo – płacowego na serwer, który następnie pobierany jest przez program Płatnik
Program Kadrowo-Płacowy	Program USOS	Jednokierunkowo z programu kadrowo – płacowego do programu USOS	Pracownicy Uniwersytetu do systemu USOS, półautomatyczny eksport pliku z systemu kadrowo-płacowego do USOS
System USOS	Program ALEPH	Jednokierunkowo z programu kadrowo – płacowego do programu bibliotecznego Aleph	Lista studentów wraz z numerem albumu, półautomatyczny eksport pliku z systemu
Program USOS	Program USOSWEB	Synchronizacja danych o studentach synchronizowane są pomiędzy systemami	Automatycznie 2 razy w ciągu doby o godzinie 16 oraz o godz. 24
Program USOS	Program OPENLDAP	Dane o autoryzacji w systemach informatycznych	Automatycznie z systemu USOS do OENLDAP dane do autoryzacji dostępu do systemu OPENLDAP – dane pracowników
Program IRK	Program USOS	Jednokierunkowo z programu IRK do programu USOS	Automatycznie pod kontrolą pracownika dziekanatu dane studentów przyjętych na studia są pobierane z IRK do USOS
Program USOS	Program APD	Jednokierunkowo z programu USOS do programu APD	Automatycznie 2 razy w ciągu doby o godzinie 16 oraz o godz. 24

System USOS	Program POLON	Jednokierunkowo z programu USOS do programu POLON	Studenci Uniwersytetu do systemu POLON, półautomatyczny eksport pliku z systemu USOS do POLON
Program kadrowo-płacowy	Program POLON	Jednokierunkowo z programu kadrowo – płacowego do programu POLON	Pracownicy Uniwersytetu do systemu POLON, półautomatyczny eksport pliku z systemu kadrowo-płacowego do POLON
System USOS	Program e-learningowy na platformie BLACKBOARD	Synchronizacja danych o studentach na zajęciach synchronizowane są pomiędzy systemami	Automatycznie 2 razy w ciągu doby o godzinie 16 oraz o godz. 24

Załacznik D

REJESTR INCYDENTÓW BEZPIECZEŃSTWA I DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH

Zadanie / problem / incydent	Zródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Czy koniec?	Odpowiedzialny za realizację	Przyczyna niezgodności	Działanie korygujące / zapobiegawcze	Ocena skuteczności

Załącznik E – Raport pokontrolny ODO	Sporządził	ABI
	Data:	
	Strona:	1 z 1

Raport nr .....

Miejsce kontroli: Kierownik kontrolowanego obszaru: Osoba(y) kontrolowane(e):	Termin wykonania kontroli: Godzina rozpoczęcia: Godzina zakończenia:
Kontrolerzy:	Kontrolowany obszar:

Podstawa auditu (zaznacz właściwe)
□ - planowa kontrola, □ - kontrola specjalna □ - kontrola sprawdzająca

Zakres	Uchybienie / spostrzeżenie / (U1, U2, U3 ... lub S1, S2, S3 ...)
Przesłanki legalności przetwarzania danych osobowych zwykłych i wrażliwych	
Zakres i cel przetwarzania danych	
Merytoryczna poprawność danych i ich adekwatność do celu przetwarzania	
Obowiązek informacyjny (art. 24) dane osobowe zbierane od osoby, której dotyczą	
Obowiązek informacyjny (art. 25) dane osobowe zbierane nie od osoby, której dotyczą	
Zgłoszenie zbioru do rejestracji	
Przekazywanie danych do państwa trzeciego	
Powierzenie przetwarzania danych	
Zabezpieczenia organizacyjne	
Zabezpieczenia fizyczne	
Zabezpieczenia infrastruktury informatycznej (informatycznej i telekomunikacyjnej)	
Zabezpieczenia infrastruktury informatycznej (baz i aplikacji z danymi osobowymi)	
Wymagania dla systemów przetwarzających dane osobowe	
Zabezpieczenia osobowe	

Kontrolowany
.....

Kontroler
.....

Załącznik F – Sprawozdanie – roczny raport stanu Systemu Ochrony Danych Osobowych	Sporządził	ABI
	Data:	
	Strona:	1 z 2

Uczestnicy przeglądu:	Termin przeprowadzenia przeglądu:

Zagadnienia omawiane na przeglądzie:	Komentarze / uwagi

Podsumowanie realizacji zadań z poprzedniego przeglądu	
Omówienie wyników kontroli przeprowadzonych *(w okresie od ostatniego przeglądu)*	
Omówienie zarejestrowanych incydentów oraz ilości i powodów ich wystąpienia *(w okresie od ostatniego przeglądu)*	
Omówienie najważniejszych działań korygujących i zapobiegawczych *(zrealizowanych i w trakcie realizacji)*	
Proponowane zadania do realizacji *(do oceny na kolejnym przeglądzie)*	

Podpisy uczestników przeglądu

Załącznik G – Plan szkolenia zakresu Ochrony Danych Osobowych

Każdy pracownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub do zbiorów w wersji papierowej winien być poddany przeszkoleniu w zakresie przepisów prawnych dotyczących ochrony danych osobowych obowiązujących przy korzystaniu z systemu informatycznego w organizacji. Za przeprowadzenie szkolenia odpowiada Administrator Bezpieczeństwa informacji, za jego zorganizowanie odpowiada przełożony szkolonych pracowników.

Szkolenie w szczególności powinno obejmować:

- Przedstawienie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wraz z późniejszymi zmianami i jej wpływu na przebieg procesów związanych z przetwarzaniem danych osobowych w Uniwersytecie, a w szczególności:
    - podstawowych definicji, w tym określenia danych osobowych, przetwarzania danych i przetwarzania danych w systemie informatycznym,
    - prawnego umocowania administratora bezpieczeństwa informacji,
    - dopuszczalności przetwarzania danych osobowych,
    - obowiązków wobec osób, których dane osobowe dotyczą,
    - praw osób, których dane osobowe dotyczą,
    - dopuszczalności udostępniania danych osobowych,
    - rejestracji zbiorów danych osobowych,
    - uprawnień GIODO, w tym uprawnień kontrolnych,
    - przepisów karnych.
- Przedstawienie rozporządzenia ministra spraw wewnętrznych i administracji z dnia 3 czerwca 1998 r. w sprawie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, a w szczególności:
    - odpowiedzialności osób przetwarzających dane osobowe,
    - postępowania w przypadku naruszenia bezpieczeństwa danych osobowych,
    - obszaru, w którym odbywa się przetwarzanie danych osobowych,
    - zasad niszczenia danych osobowych zapisanych na nośnikach informatycznych,
    - zasad zarządzania systemem informatycznym przetwarzającym dane osobowe,
    - zasad tworzenia kopii awaryjnych,
    - postępowania z wydrukami danych osobowych,
    - zasad uwierzytelniania i autoryzacji w systemie informatycznym przetwarzającym dane osobowe,
    - rozliczalności operacji w systemie informatycznym przetwarzającym dane osobowe,
- Przedstawienie innych regulacji prawnych określających zasady bezpiecznego przetwarzania danych osobowych, w tym:
    - Konwencji Rady Europy Nr 108 z dnia 28 stycznia 1991 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych,
    - właściwych dla prowadzonej przez Uniwersytet działalności rekomendacji i rezolucji Rady Europy,

- Dyrektywy 95/46/WE Parlamentu Europejskiego oraz Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnym przepływie tych danych.

- Przedstawienie podstawowych zasad ochrony danych osobowych przetwarzanych w systemie informatycznym w Uniwersytecie, a w szczególności:
  - strategii i polityki Uniwersytetu w zakresie ochrony danych osobowych przetwarzanych w systemie informatycznym,
  - odpowiedzialności za zabezpieczenie przetwarzanych danych przez użytkowników systemu informatycznego,
  - zabezpieczeń technicznych, z którymi zetkną się użytkownicy systemu informatycznego i z których będą korzystać,
  - zasad zarządzania dostępem do danych osobowych przetwarzanych w systemie informatycznym,
  - obowiązku użytkowników w zakresie zabezpieczenia i zachowania w tajemnicy użytkowanych haseł,
  - zasad ochrony antywirusowej obowiązujących w Uniwersytecie, a zwłaszcza powinności użytkowników systemu informatycznego przetwarzającego dane osobowe,
  - zasad użytkowania nośników przenośnych zawierających dane osobowe,
  - zasad bezpiecznego serwisowania sprzętu informatycznego służącego do przetwarzania i przechowywania danych osobowych,
  - zasad zabezpieczenia wydruków danych osobowych,
  - zabezpieczenia dostępności danych osobowych poprzez tworzenie kopii awaryjnych lub umożliwienie powołanym do tego pracownikom utworzenia kopii awaryjnych przetwarzanych danych osobowych,
  - zasad korzystania z komputerów przenośnych przetwarzających dane osobowe – o ile w szkolonej grupie znajdują się osoby, które będą w ten sposób przetwarzały dane osobowe,
  - sposobu reagowania na incydenty związane z utratą bezpieczeństwa danych osobowych, a zwłaszcza poinformowania administratora bezpieczeństwa informacji i zabezpieczenia dowodów incydentu,
  - konsekwencji w przypadku nieprzestrzegania zasad zabezpieczenia procesów przetwarzania danych osobowych w systemie informatycznym.

Szkolenie zostaje zakończone podpisaniem przez słuchacza dokumentu zawierającego:

- Imię i nazwisko słuchacza,
- Datę odbycia szkolenia,
- Imię i nazwisko osoby prowadzącej,
- Oświadczenie o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia i obowiązujących zasad korzystania z systemu informatycznego przetwarzającego dane osobowe oraz zasad ochrony tych danych.

Dokument ten jest przechowywany przez Administratora bezpieczeństwa informacji i stanowi podstawę do podejmowania działań w celu nadania pracownikowi uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe oraz dostępu do zbiorów w wersji papierowej.

Lista uczestników szkolenia z zakresu Ochrony Danych Osobowych

Prowadzący:

Miejsce i data szkolenia:

L.P.	Imię uczestnika	Nazwisko uczestnika	Podpis

Załącznik H - Wzór oświadczenia

.....
(imię i nazwisko)

.....
(miejscowość, data)

OŚWIADCZENIE

Oświadczam, iż zostałam/zostałem* zapoznana/zapoznany* z przepisami dotyczącymi ochrony danych osobowych, w szczególności z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2002r. Nr 101, poz. 926 ze zm.), wydanymi na jej podstawie aktami wykonawczych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych „Polityką Bezpieczeństwa Informacji" oraz „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

1. Jednocześnie oświadczam, iż jestem zatrudniony/zatrudniona* przez Rektora Uniwersytetu w Białymstoku na podstawie umowy o pracę zawartej w dniu..... r.

2. Zobowiązuję się do:
   - zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych,
   - niewykorzystywania danych osobowych w celach pozasłużbowych o ile nie są one jawne,
   - zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne,
   - przestrzegania regulaminu ochrony danych osobowych,
   - korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
   - wykorzystywania jedynie legalnego oprogramowania pochodzącego od Pracodawcy,
   - należytej dbałości o sprzęt i oprogramowanie zgodnie z regulaminem ochrony danych osobowych,
   - korzystania z komputerów przenośnych zgodnie z regulaminem ochrony danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych

.....
podpis pracownika

* niepotrzebne skreślić

Załącznik H - Oświadczenie

....
(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE (pracownika, zleceniobiorcy)*

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2002r. Nr 101, poz. 926 ze zm.), wydanymi na jej podstawie aktami wykonawczymi oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych „Polityką Bezpieczeństwa Informacji" oraz „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

Zobowiązuję się do:

- zachowania w tajemnicy: **danych osobowych** oraz danych stanowiących tajemnicę Uniwersytetu a w szczególności nieujawnionych do wiadomości publicznej: danych klientów, ofert handlowych, warunków kontraktów i umów, danych finansowych, planów strategicznych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych, lub zadań zleconych przez Pracodawcę / Zleceniodawcę,
- niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem o ile nie są one jawne,
- przestrzegania regulaminu ochrony danych osobowych,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych lub zadań zleconych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Pracodawcy / Zleceniodawcy.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę / Zleceniodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy i/lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych, lub za naruszenie tajemnicy przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jed. Dz. U. z 2003 r. Nr 153, poz. 1503).

.....
Podpis pracownika, zleceniobiorcy

* niepotrzebne skreślić