PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 40, fax. 83 344 99 50
NIP 537 213 18 53 REGON 030310705

Zarządzenie Nr 54/2015
Rektora Państwowej Szkoły Wyższej im. Papieża Jana Pawła II
w Białej Podlaskiej
z dnia 07.10.2015r.

w sprawie: zabezpieczenia danych osobowych.

Na podstawie art. 36 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jednolity: Dz. U. z 2014r., poz.1182) oraz § 3 pkt 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004r. (Dz. U. z 2004r., nr 100, poz. 1024).

§ 1

1. Wprowadza się do użytku służbowego znowelizowaną „Instrukcję Polityki Bezpieczeństwa i Ochrony Danych Osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej" w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.

2. Wprowadza się do użytku służbowego „Instrukcję Zarządzania Systemem Informatycznym Służącym do przetwarzania Danych Osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej" w brzmieniu stanowiącym załącznik nr 2 do niniejszego zarządzenia.

§ 2

Upoważnienia dotychczas wydane użytkownikom upoważniające do przetwarzania danych osobowych przed wprowadzeniem „Instrukcji.." § 1 pkt 1 i 2 zachowują swoją aktualność.

§ 3

Traci moc zarządzenie Nr 21/2010 Rektora Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej z dnia 23. 06. 2010r. w sprawie bezpieczeństwa i ochrony danych osobowych.

§ 4

Nadzór nad realizacją zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 5

Zarządzenie wchodzi w życie z dniem jego podpisania.

Prof. zw. dr hab. Józef Bergier

Rektor PSW im. Papieża Jana Pawła II
w Białej Podlaskiej

PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 40, fax. 83 344 99 50
NIP 537 213 18 53 REGON 030310705

Załącznik Nr 1 do zarządzenia Nr 54/2015r. Rektora Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej z dnia 01.10. 2015r.

POLITYKA BEZPIECZEŃSTWA

W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

W PAŃSTWOWEJ SZKOLE WYŻSZEJ im. PAPIEŻA

JANA PAWŁA II w BIAŁEJ PODLASKIEJ

Opracował
Administrator Bezpieczeństwa Informacji

.....

Biała Podlaska **2015**

Rozdział I – Część ogólna

§1

Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej zwana dalej Polityką Bezpieczeństwa określa sposób zabezpieczenia i przetwarzania danych osobowych.

§2

Ze względu na wagę problemów związanych z ochroną prawa do prywatności a w szczególności prawa osób fizycznych powierzających swoje dane osobowe do właściwej i skutecznej ochrony tych danych należy:

1. podejmować wszelkie niezbędne działania dla ochrony praw i usprawiedliwionych interesów jednostki związane z bezpieczeństwem danych osobowych;

2. podnosić świadomość oraz kwalifikacje osób przetwarzających dane osobowe w PSW w zakresie problematyki bezpieczeństwa tych danych;

3. traktować obowiązki osób zatrudnionych w PSW przy przetwarzaniu danych osobowych jako należące do kategorii podstawowych obowiązków pracowniczych;

4. stale doskonalić i rozwijać nowoczesne metody przetwarzania danych oraz podejmować i rozwijać organizacyjne, techniczne i informatyczne środki ochrony tych danych tak aby skutecznie zapobiegać zagrożeniom związanym z:

   a). nieautoryzowanym dostępem, wykradaniem bądź niszczeniem danych przez wszelkiego rodzaju mechanizmy i programy szpiegujące, wirusy komputerowe, konie trojańskie i inne niepożądane oprogramowania,

   b). dostępem do nieautoryzowanych i niebezpiecznych stron internetowych, mogących posiadać skrypty pozwalające wykradać zasoby komputera, który się z nim łączy,

   c). atakami z sieci umożliwiającymi przetwarzanie danych,

   d). użytkowaniem oprogramowania do wymiany plików mogącym służyć do łatwego skopiowania danych poza PSW,

   e). możliwością niekontrolowanego kopiowania danych na zewnętrzne nośniki,

   f). działaniami mającymi na celu zaburzenie integralności danych w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,

   g). lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez zabezpieczenia,

   h). brakiem świadomości niebezpieczeństwa przy dopuszczaniu osób postronnych do swojego stanowiska,

   i). kradzieżą sprzętu lub nośników z danymi,

   j). kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,

k). przekazywaniem sprzętu komputerowego do serwisu zewnętrznego i innymi zagrożeniami mogącymi wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

Rozdział II – Definicje

Użyte w niniejszej Polityce Bezpieczeństwa sformułowania i skróty oznaczają:

§3

1. **PSW** – Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej;

2. **Rektor** – Rektor Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej;

3. **Ustawa** – ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182);

4. **Rozporządzenie** – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.kwietnia 2004r. 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);

5. **ADO** – Administrator Danych Osobowych;

6. **ABI** – osoba wyznaczona przez administratora Danych Osobowych do pełnienia funkcji Administratora Bezpieczeństwa Informacji;

7. **ASI** – osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Systemu Informatycznego;

8. **użytkownik danych** – każdy pracownik, który wykonując czynności służbowe przetwarza dane osobowe tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie;

9. **osoba upoważniona** – osoba posiadająca upoważnienie dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu;

10. **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, połączeń sieciowych i narzędzi programowych zastosowanych w celu przetwarzania danych;

11. **system przetwarzania danych** – ta część systemu informatycznego oraz te procedury przetwarzania dokumentów papierowych, które razem tworzą system współpracujących ze sobą mechanizmów wykorzystywanych przy przetwarzaniu danych w PSW;

12. **przetwarzanie danych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, zmienianie, udostępnianie i usuwanie;

13. **integralność danych** – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

14. **poufność danych** – właściwość zapewniającą, że dane nie są udostępniane

nieupoważnionym podmiotom i osobom;

15. **zbiór danych osobowych** – każdy posiadający strukturę logiczną zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Rozdział III – Cel wprowadzenia Polityki Bezpieczeństwa

§4

Celem wprowadzenia niniejszej Polityki Bezpieczeństwa jest:

1). Ochrona danych osobowych przetwarzanych i gromadzonych w PSW i dotyczy:

a). zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci pomiędzy programami i osobami je przetwarzającymi,

b). metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,

c). procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,

d). ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,

e). określenie polityki i sposobów dostępu do tych pomieszczeń przez pracowników.

2). Zmniejszenie ryzyka utraty informacji.

3). Określenie zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych.

4). Podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych danych.

Rozdział IV – Zakres stosowania Polityki Bezpieczeństwa

§5

Zasady określone przez niniejszy dokument mają zastosowanie do całego systemu przetwarzania danych osób w PSW tj. do:

1). Istniejącego systemu informatycznego oraz papierowego, w których przetwarzane są lub będą informacje podlegające ochronie.

2). Wszystkich nośników papierowych, magnetycznych, na których są przetwarzane informacje podlegające ochronie.

3). Wszystkich lokalizacji budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

4). Wszystkich pracowników w rozumieniu kodeksu pracy, konsultantów, stażystów i innych

osób mających dostęp do informacji podlegających ochronie.

Rozdział V – Sposób i zakres udostępniania dokumentu

§6

1. Z Polityką Bezpieczeństwa powinni zapoznać się:

   1). osoby upoważnione do przetwarzania danych osobowych w zbiorach i bazach danych;

   2). pracownicy Działu Teleinformatycznego;

   3). osoby posiadające laptopy służbowe, na których są przetwarzane dane osobowe.

2. Za rozpowszechnienie dokumentu i umożliwienie zapoznania z nim pracowników PSW odpowiedzialny jest ABI.

3. Polityka Bezpieczeństwa powinna zostać umieszczona w poczcie elektronicznej do, której dostęp posiadają pracownicy PSW lub w uzasadnionych przypadkach powinna zostać przedłożona w formie papierowej.

Rozdział VI – Zasady ogólne

§7

W celu zabezpieczenia danych osobowych gromadzonych i przetwarzanych w PSW oraz w celu podniesienia bezpieczeństwa w przetwarzającym je systemie informatycznym a w szczególności w celu ochrony danych osobowych wprowadza się określone w niniejszym dokumencie zasady postępowania.

§8

PSW realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dokłada szczególnej staranności ochrony interesów osób, których dane dotyczą i zapewnia aby dane te były:

1). przetwarzane zgodnie z prawem;

2). zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;

3). merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;

4). przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§9

Polityka Bezpieczeństwa odnosi się do danych osobowych przetwarzanych w zbiorach:

1). tradycyjnych, w szczególności w kartotekach, teczkach akt personalnych, wykazach i innych zbiorach ewidencyjnych;

2). w systemie informatycznym PSW

§10

1.PSW realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną a w szczególności:

1). zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym;

2). zabraniem przez osobę nieuprawnioną;

3). przetwarzaniem z naruszeniem ustawy;

4). zmianą, utratą, uszkodzeniem lub zniszczeniem

2. Dąży do systematycznego unowocześniania stosowanych na jej terenie środków ochrony tych danych.

3. Zapewnia aktualizację informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem i innymi zagrożeniami płynącymi z funkcjonowania systemu informatycznego oraz sieci telekomunikacyjnej.

§11

1. PSW sprawuje kontrolę i nadzór nad niszczeniem zbędnych danych osobowych i ich zbiorów.

2. Niszczenie zbędnych danych osobowych lub zbiorów polegać powinno na:

1). trwałym fizycznym zniszczeniem danych wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod;

2). animizacji danych polegającej na pozbawieniu cech pozwalających na identyfikację osób fizycznych, których animizowane dane dotyczą.

3. Osoby przetwarzające dane osobowe w PSW mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych.

4. Naruszenie przez zatrudnione w ramach stosunku pracy osoby upoważnione do dostępu lub przetwarzania danych stosowanych w PSW procedur niszczenia zbędnych danych traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych ze wszystkimi wynikającymi konsekwencjami z rozwiązaniem stosunku pracy włącznie.

5. Kontrola i nadzór nad niszczeniem zbędnych danych może w szczególności polegać na wprowadzeniu odpowiednich procedur niszczenia danych a także zlecaniu niszczenia ich wyspecjalizowanym podmiotom zewnętrznym gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika danych.

§12

1. PSW w zakresie ochrony danych osobowych prowadzi dokumentację opisującą sposób przetwarzania danych w skład, której wchodzą:

1). Zarządzenia Rektora odnoszące się do kwestii bezpieczeństwa danych osobowych;

2). Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej;

3). Instrukcja Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej;

Rozdział VII – Udostępnianie danych osobowych

§13

1. PSW udostępnia przetwarzane na jej obszarze dane osobowe wyłącznie osobom do tego upoważnionym na mocy uregulowań prawnych.

2. Upoważnienie , o którym mowa w §13 pkt 1 wynikać może w szczególności:

   1). z charakteru pracy wykonywanej na danym stanowisku;

   2). z dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na stanowisku pracy;

   3). z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.

§14

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia administratora danych może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych osobowych określonej kategorii.

2. W szczególności dostęp na wskazanej w §14 pkt 1 zasadzie mogą mieć: Państwowa Inspekcja Pracy, Policja, Najwyższa Izba Kontroli, Agencja Bezpieczeństwa Wewnętrznego, Główny Inspektor Ochrony Danych Osobowych, organy skarbowe, sądy powszechne i inne upoważnione przez przepisy prawa i organy działające w granicach przyznanych im uprawnień – wszystkie po okazaniu dokumentów potwierdzające te uprawnienia.

Rozdział VIII – Osoby odpowiedzialne i przetwarzające dane osobowe

§15

1. Rektor sprawuje obowiązki Administratora Danych lub wyznacza na tę funkcję osobę w rozumieniu ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (jednolity tekst Dz. U. z 2014r. poz. 1182) a ponadto wyznacza:

   1). Administratora Bezpieczeństwa Informacji (ABI) do, którego zadań należy:

      a). określanie wagi informacji przetwarzanych w PSW w celu realizacji zadań statutowych,

      b). analiza ryzyka związanego z przetwarzaniem danych w PSW,

      c). prowadzenie dokumentacji dotyczącej ochrony danych osobowych,

      d). reagowanie na incydenty w zakresie bezpieczeństwa przetwarzanych danych

osobowych,

e). prowadzenie wewnętrznej kontroli i przesyłanie sprawozdania z niej do GIODO (raz w roku) wg art. 36c ustawy.

f). prowadzenie rejestru zbiorów danych zawierających nazwę zbioru oraz informacje o których mowa w art. 41 ust. 1 pkt 2 – 4 i 7

2). Administrator Systemu Informatycznego (ASI) do, którego zadań należy:

a). zapewnienie pomocy użytkownikom przy korzystaniu z systemu informatycznego;

b). tworzenie kopii zapasowych danych przechowywanych w systemie informatycznym;

c). aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz usuwania ich skutków;

d). zarządzanie rozwiązaniami technicznymi związanymi z ochroną systemu informatycznego;

e). kontrolowanie przestrzegania zasad bezpiecznego przetwarzania danych osobowych w systemie informatycznym;

f). prowadzenie czasowych przeglądów sprawności użytkowanego sprzętu, legalności zainstalowanego oprogramowania

3). Użytkownicy przetwarzający dane osobowe do, których zadań należy:

a). przestrzeganie zasad zachowania bezpieczeństwa podczas przetwarzania danych zarówno w formie elektronicznej jak i papierowej;

b). aktywnie uczestniczyć w szkoleniach;

c). zachowanie w ścisłej tajemnicy identyfikatorów i haseł dostępu;

d). bezwzględne wykonywanie poleceń ADO, ABI i ASI w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego;

e). niedopuszczanie osób nieuprawnionych do urządzeń na ,których są przetwarzane dane osobowe.

Rozdział IX – Procedury rozpoczęcia, zawieszenia pracy przy komputerze

§16

1. Przed rozpoczęciem pracy użytkownik powinien sprawdzić czy stan sprzętu komputerowego nie wskazuje na próbę uruchomienia komputera przez osobę niepowołaną.

2. Użytkownicy uzyskują bezpośredni dostęp do systemu informatycznego jak i do danych w aplikacji po podaniu identyfikatora i właściwego hasła.

3. W przypadku bezczynności użytkownika w pracy na komputerze przez okres dłuższy niż 15 min. Automatycznie włączany jest wygaszacz ekranu.

4. Kończąc pracę użytkownik powinien:

1). zamknąć programy oraz wylogować się z systemu i wyłączyć komputer wraz z drukarką;

2). sprawdzić czy pozostawione stanowisko jest prawidłowo zabezpieczone i czy nie stwarza jakichkolwiek zagrożeń do uruchomienia go przez osoby postronne;

3). sprawdzić czy w napędach komputera nie pozostały nośniki zawierające dokumenty lub informacje zawierające dane osobowe do, których wgląd mają osoby uprawnione PSW.

Rozdział X – Prawa osób, których dane są przetwarzane

§17

1. PSW gwarantuje osobom fizycznym, których dane osobowe są przetwarzane w związku z realizacją jej statutowych celów, zapewnienie uprawnień wynikających z przepisów prawa.

2. Każdej osobie fizycznej, której dane osobowe są przetwarzane w związku z realizacją celów statutowych uczelni, przysługuje prawo do uzyskania informacji o ich uprawnieniach związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzania danych, które jej dotyczą zawartych w zbiorach danych na zasadach określonych w rat. 32 – 35 ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych.

3. Osoby fizyczne, których dane osobowe są przetwarzane uzyskują informacje o przysługujących im prawach w sposób przyjęty w PSW.

Rozdział XI – Wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych

§18

1. Dane osobowe, które leżą w gestii administrowania i gromadzenia przez PSW są przetwarzane w budynkach uczelni nr 102, 95/97, 105 i 107/111 przy ul. Sidorskiej w Białej Podlaskiej.

2. W szczególnie uzasadnionych przypadkach możliwe jest przetwarzanie danych osobowych na komputerach przenośnych wyłącznie za zgodą ADO.

3. Dostęp do budynków i pomieszczeń , w których są przetwarzane dane osobowe podlega kontroli.

4. Kontrola dostępu polega w szczególności na ewidencjonowaniu pobierania i zwrotu kluczy od pomieszczeń przez osoby upoważnione do przetwarzania danych osobowych w tych pomieszczeniach.

Rozdział XII – Zbiory danych osobowych tworzone w PSW

§19

1. PSW realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych tworzonych na jego obszarze.

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem:

1). struktury zbiorów;

2). zawartości poszczególnych pól informacyjnych i powiązań między nimi;

3). programów zastosowanych do przetwarzania tych danych.

§20

PSW zgodnie z przepisami ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych zapewnia ochronę zbiorom danych osobowych sporządzanym doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką realizowaną w Uczelni, a po ich wykorzystaniu niezwłocznie usuwanych.

§21

Zabrania się tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne do realizacji celów statutowych PSW.

Rozdział XIII – Postanowienia końcowe

§22

Polityka Bezpieczeństwa jest dokumentem wewnętrznym PSW.

§23

Wszyscy pracownicy upoważnieni do przetwarzania danych osobowych zobowiązani są do zapoznania się z treścią niniejszej polityki.

§24

1. Wykazy, zasady i rejestr zbiorów znajdujące się w załącznikach 1 - 4 i 6 - 11 do Polityki prowadzi ABI.

2. Wykaz znajdujący się w załączniku nr 5 do Polityki prowadzi w zakresie środków organizacyjnych ABI, zaś w zakresie środków technicznych ASI.

§25

Integralną część niniejszej Polityki Bezpieczeństwa stanowią następujące załączniki:

1) załącznik nr 1 – Rejestr zbiorów w PSW;

2). załącznik nr 2 – Rejestr osób upoważnionych do przetwarzania danych osobowych w PSW;

3). załącznik nr 3 – Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;

4). załącznik nr 4 – Wykaz budynków, pomieszczeń tworzących obszar, w których są przetwarzane dane osobowe;

5). załącznik nr 5 – Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w PSW;

6). załącznik nr 6 – Opis struktury zbioru ze wskazaniem programu zastosowanego do

przetwarzania danych osobowych;

7). załącznik nr 7 – Zasady korzystania z komputerów przenośnych (laptopów), na których są przetwarzane dane osobowe;

8). załącznik nr 8 – Zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w PSW;

9). załącznik nr 9 – Oświadczenie;

10. załącznik nr 10 – Upoważnienie;

11. załącznik nr 11 – Odwołanie upoważnienia.

§26

Jakiekolwiek zmiany wprowadzone w załącznikach do niniejszego dokumentu nie wymagają zmiany zarządzenia, które wprowadziło Politykę Bezpieczeństwa w życie.

§27

Polityka Bezpieczeństwa wchodzi w życie z dniem podpisania zarządzenia przez Rektora.

Załącznik nr 1 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

Rejestr Zbiorów w PSW w Białej Podlaskiej

Rejestr zbiorów powinien zawierać następujące pozycje:

1. liczbę porządkową,
2. nazwę zbioru,
3. datę założenia ,
4. oznaczenie administratora danych,
5. oznaczenie przedstawiciela AD (art.31 ustawy),
6. opis kategorii osób, których dane są przetwarzane w zbiorze,
7. sposób zbierania d. o. do zbioru,
8. sposób udostępniania d. o. ze zbioru,
9. oznaczenie odbiorcy danych, którym, którym d. o. mogą być przekazywane,
10. datę aktualizacji.

Załącznik nr 2 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

Rejestr osób upoważnionych do przetwarzania danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej

Lp.	Imię i nazwisko	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data Przyznania uprawnień	Podpis ABI PEFS	Data odebrania uprawnień	Podpis ABI PEFS 2007

Załącznik nr 3 do Polityki Bezpieczeństwa
PAW w Białej Podlaskiej

Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych

Oświadczam, że zapoznałem się z:

- Przepisami ustawy z Dia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.) oraz przepisami wykonawczymi do tej ustawy,

- Polityką Bezpieczeństwa PSW w Białej Podlaskiej i Instrukcją Zarządzania Systemem Informatycznym służącym do Przetwarzania Danych Osobowych w PSW w Białej Podlaskiej

Lp.	Imię i nazwisko	Data	Podpis potwierdzający zapoznanie się z dokumentami

Załącznik nr 4 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których są przetwarzane dane osobowe w PSW w Białej Podlaskiej

Lp.	Budynek – dane adresowe	Pomieszczenie

Załącznik nr 5 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczności ochrony danych osobowych w PSW w Białej Podlaskiej.

I. Środki ochrony fizycznej danych osobowych:

a). klucze od pomieszczeń wydawane są wyłącznie osobom upoważnionym,

b). podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz,

c). urządzenia, dyski lub inne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu danych a w przypadku gdy nie jest to możliwe uszkadza się w sposób uniemożliwiający ich odczytanie,

d). zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej szafie,

e). kopie zapasowe zbioru danych osobowych są przechowywane w zamkniętej szafie,

f). dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

II. Środki sprzętowe, informatyczne i telekomunikacyjne:

a). sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci internetowej poprzez zastosowanie firewalla programowego chroniącego zasoby PSW,

b). oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy,

c). dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła,

d). zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe.

III. Środki organizacyjne:

a). osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

b). osoby zatrudnione przy przetwarzaniu danych osobowych zostały

Załącznik nr 6 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

Opis struktury zbiorów ze wskazaniem programu zastosowanego do przetwarzania danych osobowych

Program WF – Gang

Nazwisko .....

Imię .....

Imię ojca .....

Imię matki .....

Nazwisko panieńskie .....

Numer PESEL .....

Numer dowodu osobistego .....

Adres zamieszkania: miejscowość .....

Nr domu/ lokalu.....nr mieszkania .....

Kod pocztowy.....województwo.....

Urząd skarbowy .....

Numer NIP .....

Załącznik nr 7 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe poza PSW

Przetwarzanie danych osobowych na służbowych komputerach przenośnych PSW powinno być ograniczone do niezbędnego minimum i może się odbywać wyłącznie zgody ADO .
Zakres i miejsce przetwarzania powinno być uzgodnione z ABI oraz ASI PSW.

Pracownik korzystający z komputera przenośnego do przetwarzania danych osobowych lub dokumentów stanowiących tajemnicę służbową zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

W związku z powyższym użytkownik komputera przenośnego zobowiązany jest do:

1). przechowywania przedmiotowych danych na dysku zabezpieczonym hasłem co najmniej 8-mio znakowym zawierającym duże i małe litery, znaki specjalne lub cyfry,

2). transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia a w szczególności:

a). transportu komputera w odpowiedniej, przeznaczonej do tego celu torbie jako bagażu podręcznego,

b). nie pozostawiania komputera w samochodzie, przechowalni bagażu, środkach transportu publicznego itp.,

3). korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione,

4). zdecydowanego uniemożliwienia korzystania z komputera osobom niepowołanym (np. dzieciom, znajomym),

5). zabezpieczenia komputera przenośnego hasłem i utrzymanie konfiguracji oprogramowania systemowego w stanie wymuszającym korzystanie z tego hasła,

6). zmiany hasła zgodnie z harmonogramem przyjętym w PSW,

7). blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,

8). regularnego i częstego kopiowania danych przetwarzanych na komputerze przenośnym, do systemu informatycznego PSW w celu umożliwienia wykonania kopii awaryjnej,

Załącznik nr 8 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

Zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych

1. Osoba, która zauważyła niepokojące zdarzenie, wystąpienie poniżej wymienionych symptomów lub innych objawów, które jej zdaniem mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i ubezpieczeństwa, zobowiązana jest do natychmiastowego poinformowania ABI, ASI lub ADO.

2. Informacja o pojawieniu się zagrożenia winna być przekazana przez użytkownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.

3. Naruszeniu ochrony danych osobowych mogą świadczyć symptomy występujące w następujących obszarach?:

   1). w obrębie pomieszczeń, szaf lub innych miejsc przechowywania:

      a). ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych,

      b). włamanie lub próby włamania do szaf, w których przechowywane są w postaci elektronicznej lub papierowej nośniki danych osobowych.

   2). w obrębie sprzętu informatycznego:

      a). kradzież komputera, w którym przechowywane są dane osobowe,

      b). rozkręcona obudowa komputera.

   3). w obrębie systemu informatycznego i aplikacji:

      a). brak możliwości uruchomienia aplikacji pozwalającej na dostęp do danych osobowych,

      b). brak możliwości zalogowania się do tej aplikacji,

      c). ograniczone w stosunku do normalnej sytuacji, uprawnienia użytkownika w strukturze aplikacji (brak możliwości wykonania operacji normalnie dostępnych),

      d). inny zakres lub różnice w zawartości zbioru danych osobowych dla użytkownika,

   4). inne:

      a). zagubienie lub kradzież nośnika z zawartością danych osobowych.

4. Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w PSW naruszenia bezpieczeństwa danych osobowych, ABI we współpracy z ASI jest zobowiązany do podjęcia następujących kroków:

1).stwierdzenia czy rzeczywiście doszło do naruszenia ochrony danych osobowych, w tym:

a). sprawdzenia okoliczności zdarzenia,

b). wyjaśnienia jego przyczyn, w szczególności gdy zdarzenie było związane z celowym działaniem użytkownika bądź osób trzecich.

2). w przypadku gdy doszło do naruszenia ochrony danych osobowych to:

a). zebranie ewentualnych dowodów,

b). zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,

c). zabezpieczenia danych przetwarzanych w systemie informatycznym, jego logów systemowych i bazy, w których nastąpiło naruszenie bezpieczeństwa oraz danych konfiguracyjnych całego systemu w celu późniejszej analizy,

d). usunięcia skutków incydentu i przywrócenia pierwotnego stanu systemu informatycznego tj. stanu sprzed incydentu, polegające na:

- przeprowadzeniu analizy spójności danych osobowych przetwarzanych w systemie,

- ewentualnym odtworzeniu kopii zapasowych danych i plików konfiguracyjnych,

- przeprowadzeniu analizy poprawności funkcjonowania systemu,

- powtórnym zabezpieczeniu danych przetwarzanych w systemie informatycznym, szczególnie danych konfiguracyjnych tego systemu.

4. System informatyczny PSW, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

5. ABI określa, na podstawie zebranych informacji przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym PSW.

6. ABI prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

1). imię i nazwisko osoby zgłaszającej incydent,

2). imię i nazwisko osoby przyjmującej zgłoszenie incydentu,

3). datę zgłoszenia incydentu,

4). przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,

5). wyniki przeprowadzających działań,

6). podjęte akcje naprawcze i ich skuteczność.

7. ABI odpowiedzialny jest za przeprowadzenie raz w roku analizy zaistniałych incydentów w celu:

1). określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,

2). określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego minimalizujących ryzyko zaistnienia incydentów,

3). określenia potrzeb w zakresie szkoleń ASI i użytkowników systemu informatycznego przetwarzających dane osobowe.

Załącznik nr 9 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

.....
imię i nazwisko

.....
Stanowisko

OŚWIADCZENIE

Ja niżej podpisany/a/ oświadczam, że zapoznałem/am/ się z:

1. Przepisami ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. Z 2002r. nr 101, poz. 926 z późn. zm.) oraz przepisami wykonawczymi do niej;

2. Polityką Bezpieczeństwa w Zakresie Ochrony Danych Osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej.

Jednocześnie oświadczam, że:

- zachowam w tajemnicy wszystkie informacje dotyczące danych osobowych;

- zapewnię bezpieczeństwo i ochronę danych osobowych przetwarzanych w programie;

- natychmiast zgłoszę ABI_____ stwierdzenie faktu próby naruszenia ochrony danych w systemie informatycznym.

.....
data

.....
podpis

Załącznik nr 10 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

U P O W A Ż N I E N I E Nr...../.....

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182) upoważniam:

Pana/Panią..... .....

z dniem.....

w systemie informatycznym funkcjonującym Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej.

Upoważnienie obowiązuje na okres zatrudnienia lub do dnia jego odwołania.

1. Zakres przetwarzania danych osobowych.....

.....

2. Sposób przetwarzania danych: papierowy/informatyczny*

3. Obszar przetwarzanych danych osobowych: budynek, piętro, nr pokoju.....

.....

.....
Czytelny podpis Administratora Danych lub osoby upoważnionej do wydawania i odwoływania upoważnień.

*niepotrzebne skreślić

Załącznik nr 11 do Polityki Bezpieczeństwa
PSW w Białej Podlaskiej

ODWOŁANIE UPOWŻNIENIA Nr .....
DO PRZETWARZANIA DANYCH OSOBOWYCH
W PROGRAMIE.....

Z dniem .....r. na podstawie art. 37 w związku z art. 31 ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych (Dz. U. z 2014r. poz.1182 tekst jednolity) odwołuję upoważnienie Pani/Panu..... do przetwarzania danych osobowych w systemie elektronicznym /papierowym w programie.....Państwowej Szkoły Wyższej im.Papieża Jana Pawła II w Białej Podlaskiej.

.....
Czytelny podpis Administratora Danych

PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 40, fax. 83 344 99 50
NIP 537 213 18 53 REGON 030310705

Załącznik Nr2 do zarządzenia Nr 54/2015 Rektora Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej z dnia 07. 10. 2015r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W PAŃSTWOWEJ SZKOLE WYŻSZEJ im. PAPIEŻA JANA PAWŁA II W BIAŁEJ PODLASKIEJ

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

.....

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

.....

.....

BIAŁA PODLASKA 2015r.

I. POSTANOWIENIA OGÓLNE.

Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. – tekst jednolity) oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z późn. zm.) nakłada na Administratora Danych następujące obowiązki:

- zapewnienie bezpieczeństwa i poufności danych osobowych, w tym zabezpieczenie ich przed ujawnieniem,

- zabezpieczenie danych osobowych przed nieuprawnionym dostępem,

- zabezpieczenie danych osobowych przed udostępnieniem osobom nieupoważnionym,

- zabezpieczenie przed utratą danych osobowych,

- zabezpieczenie przed uszkodzeniem lub zniszczeniem danych osobowych oraz przed ich nielegalną modyfikacją.

Instrukcja określa ramowe zasady właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne jakim powinny odpowiadać urządzenia i system informatyczny odpowiednio do zagrożeń i kategorii danych objętych ochroną.

II. PRZEZNACZENIE I TERMINY UŻYWANE W INSTRUKCJI.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej zwana dalej instrukcją określa sposób zarządzania oraz zasady administrowania systemem informatycznym służącym do przetwarzania danych.

Terminy:

1). **Administrator Danych** rozumie się przez to Rektora lub osobę upoważnioną przez Rektora.

2). **Dane osobowe** to każda informacja dotycząca osoby fizycznej pozwalająca na określenie tożsamości tej osoby.

3). **Hasło** to ciąg znaków literowych, cyfrowych lub innych znany jedynie osobie uprawnionej do pracy w systemie.

4). **Identyfikator użytkownika** to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

5). **Zbiór danych** to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy

zestaw jest rozproszony czy podzielony funkcjonalnie.

6). **Przetwarzanie danych** to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie wykonywane w systemie informatycznym.

7). **Usuwanie danych** to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

8). **Administrator Bezpieczeństwa Informacji (ABI)** to osoba wyznaczona przez Rektora odpowiedzialna za bezpieczeństwo danych osobowych w uczelni.

9). **Administrator Systemu Informatycznego (ASI)** to osoba wyznaczona przez Rektora odpowiedzialna za zarządzanie systemem informatycznym funkcję tę pełni Kierownik Działu Teleinformatycznego Uczelni.

10). **System informatyczny** to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w dziale teleinformatycznym w celu przetwarzania danych.

11). Użytkownik systemu to osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym.

12). **Obszar kontrolowany** to obszar znajdujący się pod ochroną o ograniczonym dostępie osób nieautoryzowanych, w którym odbywa się przetwarzanie danych, w tym danych osobowych.

Niniejsza instrukcja zarządzania systemem informatycznym określa:

a). poziom bezpieczeństwa danych osobowych w systemie informatycznym;

b). procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym;

c). stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem;

d). sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności;

e). procedury rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników systemu;

f). metody i częstotliwość tworzenia kopii awaryjnych;

g). metody i częstotliwość sprawdzania obecności wirusów komputerowych i metody ich usuwania;

h). sposób , miejsce i okres przechowywania;

- elektronicznych nośników informacji zawierających dane osobowe,

- kopii zapasowych.

i). sposób dokonywania przeglądów , konserwacji systemu i zbiorów danych osobowych;

j). sposób postępowania w zakresie komunikacji w sieci komputerowej;

k). procedury wykonywania przeglądów i konserwacji systemu i nośników informacji służących do przetwarzania danych osobowych.

III. OKREŚLENIE POZIOMU BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM.

1. Z analizy zagrożeń wynika, że w Uczelni miejscami najbardziej zagrożonymi są pomieszczenia budynku rektoratu, w których znajdują się zbiory danych osobowych pracowników uczelni i studentów gromadzone w kartotekach i urządzeniach służących do przetwarzania tych danych, do których mogą mieć nieuprawniony dostęp osoby nieupoważnione spoza uczelni i z uczelni.

2. Do innych zagrożeń, na które może być narażone przetwarzanie danych osobowych należy zaliczyć:

- oszustwo, kradzież, sabotaż;

- zdarzenia losowe (pożar, zalanie);

- zaniedbania pracowników uczelni (niedyskrecja, udostępnienie d. o. osobie nieupoważnionej);

- niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;

- pokonanie zabezpieczeń fizycznych;

- podglądy;

- brak rejestrowania udostępniania danych osobowych;

- niewłaściwe miejsce i sposób przechowywania dokumentacji;

- nie przydzielenie użytkownikom systemu informatycznego identyfikatorów;

- niewłaściwa konfiguracja systemu;

- zniszczenie (sfałszowanie) kont użytkowników;

- pokonanie zabezpieczeń programowych;

- kradzież danych kont;

- niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych;

- naprawy i konserwacje systemu i sieci teleinformatycznej wykonywane przez osoby nieuprawnione;

- przypadkowe bądź celowe wprowadzanie zmian do chronionych danych osobowych;

- brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

IV. ZASADY REJESTROWANIA I WYREJESTROWANIA UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO, ZAKRES ODPOWIEDZIALNOŚCI ADMINISTRATORA.

1. Rejestracji i wyrejestrowania użytkownika systemu informatycznego dokonuje upoważniony przez Rektora Administrator Bezpieczeństwa Informacji.

2. Każdy użytkownik upoważniony do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe winien posiadać własny odrębny identyfikator i hasło dostępu.

3. Rozwiązanie stosunku pracy, bądź zmiana zakresu obowiązków powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu oraz wykreślenie z ewidencji.

V. ZASADY DOPUSZCZANIA PRACOWNIKÓW DO EKSPLOATACJI SYSTEMU INFORMATYCZNEGO PRZETWARZAJĄCEGO ZBIORY DANYCH OSOBOWYCH.

1. Do obsługi systemu informatycznego Uczelni oraz urządzeń wchodzących w jego skład, służących do zbierania lub przetwarzania danych osobowych mogą być dopuszczeni wyłącznie pracownicy posiadający aktualne, ważne upoważnienia.

2. Administrator Bezpieczeństwa Informacji zapoznaje pracowników z przepisami ochronie danych osobowych oraz wykazem akt i wiadomości stanowiących tajemnicę służbową(w zakresie ochrony danych osobowych).

VI. ZASADY TWORZENIA I POSŁUGIWANIA SIĘ HASŁAMI DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym Uczelni użytkownik może mieć wyłącznie po podaniu identyfikatora i oraz właściwego hasła.

2. Należy wybierać hasła, które:
   - nie są hasłami słownikowymi;
   - składają się z co najmniej sześciu znaków;
   - zawierają zarówno duże jak i małe litery, cyfry oraz inne znaki.

3. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.

4. Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.

5. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.

6. Użytkownicy nie mogą korzystać z innych identyfikatorów niż tego do , którego są przypisani.

VII. PROCEDURY ROZPOCZĘCIA, KONTYNUOWANIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM.

1. Użytkownik rozpoczynający pracę zobowiązany jest do sprawdzenia zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz sprzętu komputerowego, na którym pracuje.

2. Przed rozpoczęciem pracy i w trakcie każdy użytkownik jest zobowiązany do zwracania bacznej uwagi, czy nie wystąpiły objawy mogące świadczyć o naruszeniu zasad ochrony danych osobowych.
   Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

3. Krótkotrwałe przerwy w pracy (bez opuszczania stanowiska pracy) nie wymagają zamykania aplikacji.

4. Odchodząc od swojego komputera każdy użytkownik powinien aktywować wygaszacz ekranu zabezpieczony hasłem dostępu.

5. Przed całkowitym opuszczeniem stanowiska pracy użytkownik obowiązany Jest zamknąć aplikację i wylogować się z pracy w sieci.

6. Zakończenie pracy polega na zamknięciu wszystkich programów (programu). Użytkownik powinien zaczekać przy komputerze do chwili jego wyłączenia.

7. Pomieszczenia, w których są przetwarzane dane osobowe po zakończeniu pracy zamyka się na klucz i klucze zdaje się do portierni.

VIII. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMÓW I URZĄDZEŃ SŁUŻĄCYCH DO ICH PRZETWARZANIA.

1.Za sporządzanie kopii zapasowych zbiorów danych osobowych odpowiedzialny jest użytkownik systemu informatycznego służącego do przetwarzania danych osobowych. Procedura tworzenia kopii zapasowych obejmuje wszystkie

komputery, na których przetwarzane są dane osobowe.

2. Nośniki z nagranymi kopiami zapasowymi przechowywane są w szafach zamykanych na klucz.

3. Kopie zapasowe powinny być kontrolowane przez Administratora Systemu Informatycznego w szczególności pod kątem ich wykonania. Nieprzydatne nośniki należy uszkodzić w sposób uniemożliwiający odczyt danych osobowych.

4. Kopie awaryjne może tworzyć Administrator Systemu Informatycznego.

IX. ZASADY NISZCZENIA I SPOSOBY DOKUMENTOWANIA PROCESU NISZCZENIA NOSNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE.

1. Nośniki zawierające kopie z danymi osobowymi po ustaniu ich użyteczności podlegają likwidacji poprzez pozbawienie ich zapisu tych danych, a gdy nie jest to możliwe, nośniki uszkadza się fizycznie w sposób uniemożliwiający odczytanie zapisanych danych poprzez rozdrobnienie lub spalenie. Z tych czynności ASI sporządza protokół.

2. Nośniki papierowe (wydruki) nie przeznaczone do ponownego użytku oraz nie archiwizowane powinny być natychmiast niszczone.

X. OKREŚLENIE ZASAD ZABEZPIECZENIA ORAZ WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH.

1. Z uwagi na fakt iż niektóre wykorzystywane komputery przetwarzające Dane osobowe posiadają dostęp do sieci publicznej, Administrator Systemu Informatycznego powinien wdrożyć procedury oraz oprogramowanie, które chroni dane osobowe przed nieuprawnionym dostępem, zmianom, usunięciem lub uszkodzeniem. Zagrożenia te to wirusy oraz ataki hakerów.

2. We wszystkich komputerach zainstalowanych w PSW są instalowane wyłącznie legalne oprogramowania posiadające licencję, certyfikat legalności itp.

3. Zabronione jest pobieranie oraz instalowanie bez nadzoru osoby upoważnionej przez ABI jakichkolwiek programów na komputerach służących do przetwarzania danych osobowych.

4. Zabronione jest również używanie nośników informacji nie pochodzących z zasobów ASI.

5. Każda osoba przetwarzająca dane osobowe przy użyciu komputera została pouczona by w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych poinformowała o tym fakcie ABI.

6. Za legalność użytkowanego oprogramowania specjalistycznego odpowiada

użytkownik systemu.

7. Do usuwania wirusów należy używać programów antywirusowych pozostających w dyspozycji Uczelni.

XI. ZABEZPIECZENIE PRZED DZIAŁANIEM OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.

Dla potrzeb systemu informatycznego w PSW stosowane jest zabezpieczenie antywirusowe dla:

- ochrony poczty ,

- skanowania ruchu internetowego,

- kontroli zmian w systemie plików,

- monitorowania procesów pamięci,

- monitorowania zmian w rejestrze systemowym,

- przywracania systemu.

XII. POSTEPOWANIE W ZAKRESIE KOMUNIKACJI SIECIOWEJ.

1. Przeglądarka (jeżeli jest to możliwe) powinna mieć ustawione opcje tak, by nie zapamiętywała nazwy użytkownika oraz hasła.

2. Komunikacja w sieci komputerowej dozwolona jest tylko po odpowiednim zalogowaniu się i podaniu indywidualnego hasła użytkownika.

3. Dostęp do wszystkich folderów i plików z sieci zabezpieczony jest odpowiednimi uprawnieniami.

XIII. POSTANOWIENIA KOŃCOWE.

1. Każda osoba wpisana do ewidencji zobowiązana jest do odbycia stosownego przeszkolenia w zakresie ochrony danych osobowych oraz zapoznania się z:

   - treścią ustawy i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dna 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

   - polityką bezpieczeństwa w zakresie ochrony danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej;

- niniejszą instrukcją i uregulowaniami wewnętrznymi obowiązującymi w tym zakresie.

2. Wszelkie zagadnienia dotyczące ochrony danych osobowych nie ujęte w tej „Instrukcji" należy rozpatrywać zgodnie z treścią aktów prawnych dotyczących ochrony danych osobowych z uwzględnieniem późniejszych zmian uzupełnień.