PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 00, fax 83 344 99 50
NIP 537-21-31-853 REGON 030310705

Zarządzenie nr 32/2018

Rektora Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej z dnia 20.06.2018r.

w sprawie: **wprowadzenia „ Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej" o treści zgodnej z załącznikiem**

§1

Wprowadza się do użytku służbowego znowelizowaną „ Politykę bezpieczeństwa w zakresie ochrony danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej" dostosowaną do wymogów rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/16/WE (ogólne rozporządzenie o ochronie danych Dz.UEL.2016.119.1-dalej RODO).

§2

Upoważnienia do przetwarzania danych osobowych wydane użytkownikom upoważniające do przetwarzania do 24.maja 2018r. zachowują swoją aktualność.

§3

Traci moc 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.

§4

Nadzór nad realizacją zarządzenia powierzam Inspektorowi Ochrony Danych Osobowych (IODO) w osobie Pana Jana Sroki.

§5

Zarządzenie wchodzi w życie w ciągu 14 dni od jego podpisania.

prof. dr hab. Józef Bergier

Rektor PSW im. Papieża Jana Pawła II w Białej Podlaskiej

Załącznik:

Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Państwowej Szkole Wyższej 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 00, fax 83 344 99 50
NIP 537-21-31-853 REGON 030310705

Załącznik do Zarządzenia nr 32/2018r.
Rektora Państwowej Szkoły Wyższej im. Papieża Jana
Pawła II w Białej Podlaskiej
z dnia 20.06.2018r.

POLITYKA BEZPIECZEŃSTWA
W ZAKRESIE OCHRONY DANYCH OSOBOWYCH
W PAŃSTWOWEJ SZKOLE WYŻSZEJ IM. PAPIEŻA
JANA PAWŁA II W BIAŁEJ PODLASKIEJ

Opracował

Inspektor Ochrony Danych Osobowych

Jan Sroka

Biała Podlaska, 2018 r.

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, atakami z sieci umożliwiającymi przetwarzanie danych,
   c. użytkowaniem oprogramowania do wymiany plików mogącym służyć do łatwego skopiowania danych poza PSW,
   d. możliwością niekontrolowanego kopiowania danych na zewnętrzne nośniki,
   e. działaniami mającymi na celu zaburzenie integralności danych w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
   f. lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez zabezpieczenia,
   g. brakiem świadomości niebezpieczeństwa przy dopuszczaniu osób postronnych do swojego stanowiska,
   h. kradzieżą sprzętu lub nośników z danymi,
   i. kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,
   j. 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. Rozporządzenie Parlamentu Europejskiego i Rady EU 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

4. Ustawa z dnia 10 maja o ochronie danych osobowych (Dz. U. z 2018r., poz1000).

5. 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);

6. ADO - Administrator Danych Osobowych (Rektor)

7. IODO – Inspektor Ochrony Danych Osobowych osoba wyznaczona przez ADO i zgłoszona do Urzędu Ochrony Danych Osobowych

8. ASI - osoba przeszkolona wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Systemu Informatycznego;

9. 0soba upoważniona - osoba posiadająca upoważnienie dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym i tradycyjnym

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 zapewniająca, że dane nie są udostępniane

nieupoważnionym podmiotom i osobom;

15. Dane osobowe- wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej bezpośrednio lub pośrednio na podstawie identyfikatora jak imię i nazwisko, lokalizacja, identyfikator internetowy itp.

16. 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.

17.Profilowanie –dowolna forma przetwarzania danych osobowych polegająca na ich wykorzystaniu do oceny niektórych czynników osobowych osoby fizycznej do analizy lub prognozy efektów pracy, sytuacji ekonomicznej, zdrowia, preferencji, zainteresowań, wiarygodności, lokalizacji lub przemieszczania się.

18. Pseudonimizacja – przetwarzanie danych osobowych w taki sposób, by nie można było ich przypisać konkretnej osobie, której dane dotyczą bez użycia dodatkowych informacji pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

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;
5) osób mających dostęp do informacji podlegających ochronie;

Rozdział V - Sposób i zakres udostępniania dokumentu

§6

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.

1. Za rozpowszechnienie dokumentu i umożliwienie zapoznania z nim pracowników PSW odpowiedzialny jest IODO.

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. Do zasad tych należy:

1). informowanie Inspektora Ochrony Danych Osobowych przez kadry /kierowników jednostek organizacyjnych/ o zwolnieniu lub zmianie stanowiska przez pracownika;

2). Administrator Systemu Informatycznego bez zbędnej zwłoki cofa uprawnienia dostępu do danych osobowych lub usługi w systemie informatycznym PSW.

§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 RODO;
   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;
2. Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania d.o. danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej.
3. Rejestr kategorii zbiorów danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej.
4. Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych w państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej podlaskiej.
5. Rejestr czynności przetwarzania danych osobowych w państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej podlaskiej (art.30, ust.1 RODO).

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 unijnego lub prawa państwa członkowskiego.

Rozdział VIII - Osoby odpowiedzialne i przetwarzające dane osobowe

§15

1. Rektor sprawuje obowiązki Administratora Danych Osobowych zgodnie z RODO wyznacza:

1). Inspektora Ochrony Danych Osobowych 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 raz w roku dla Administratora;
f) prowadzenie rejestru zbiorów danych zawierających nazwę zbiorów

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

a) zapewnienie pomocy przetwarzającym 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

2. 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, IODO 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.
4) zabezpieczyć dokumentacje tradycyjną w szafach.
5) o wszelkich podejrzeniach naruszenia bezpieczeństwa w zakresie ochrony danych osobowych informować bez zbędnej zwłoki IODO Iasi.

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 praw wynikających z przepisów rodo.
2. Każdej osobie fizycznej, której dane osobowe są przetwarzane w związku z realizacją celów statutowych uczelni, przysługuje prawo do uzyskania informacji o ich danych,
3. Osobie ,której dane są przetwarzane przysługuje prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych osobowych.

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, 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. Prowadzi „Rejestr kategorii i zbiorów danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej".

§20

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

§21

Polityka Bezpieczeństwa jest dokumentem wewnętrznym PSW.

§22

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

§23

1. Wykazy, zasady i rejestry znajdujące się w załącznikach do Polityki prowadzi IODO.

§24

Integralną część niniejszej Polityki Bezpieczeństwa stanowią następujące załączniki:

1) załącznik nr 1 — Rejestr osób upoważnionych do przetwarzania danych osobowych w PSW;
2) załącznik nr 2 — Wykaz budynków, pomieszczeń tworzących obszar, w których są przetwarzane dane osobowe;

3)	załącznik nr 3	Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w PSW;
4)	załącznik nr 4	Zasady korzystania z komputerów przenośnych (laptopów), na których są przetwarzane dane osobowe;
5)	załącznik nr 5	Upoważnienie do przetwarzania danych osobowych;
6)	załącznik nr 6	Odwołanie upoważnienia;
7)	załącznik nr 7	Wniosek o nadanie upoważnienia do przetwarzania danych osobowych;

§25

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

§26

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

Otrzymują:

-Prorektor ds. nauczania

- kierownicy jednostek organizacyjnych;

- Kanclerz

- dział kadr;

- Kwestor.

REKTOR

prof. dr hab. Józef Bergier

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 IODO	Data odebrania uprawnień	Podpis IODO

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

Lp.	Budynek – dane adresowe	Pomieszczenie

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 upoważnione do przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

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 za zgodą ADO.

Zakres i miejsce przetwarzania powinno być uzgodnione z 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 identyfikatorem 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
6) oprogramowania systemowego w stanie wymuszającym korzystanie z tego hasła,
7) zmiany hasła zgodnie z harmonogramem przyjętym w PSW,
8) blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,
9) regularnego i częstego kopiowania danych przetwarzanych na komputerze przenośnym, do systemu informatycznego PSW w celu umożliwienia wykonania kopii awaryjnej,

UPOWAŻNIENIE

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r. w2 sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/16/WE (ogólne rozporządzenie o ochronie danych Dz.UEL.2016.119.1-dalej RODO) niniejszym upoważniam do przetwarzania danych osobowych:

Pan/a/nią imię i nazwisko do przetwarzania danych osobowych.....

W następującym zbiorze /zbiorach:

.....

.....

.....

Upoważnienie ważne jest od..... do.....

.....

Czytelny podpis administratora / nadającego upoważnienie

Ja niżej podpisana oświadczam, że zapoznała/em się z:

1. Polityką Bezpieczeństwa Ochrony Danych Osobowych w PSW w Białej Podlaskiej.

Jednocześnie oświadczam, że:

- zachowam w tajemnicy wszystkie informacje dotyczące danych osobowych;
- zapewnię bezpieczeństwo i ochronę danych przetwarzanych w programie;
- natychmiast zgłoszę do IODO .....e-mail: j.sroka@pswbp.pl stwierdzenie faktu naruszenia ochrony danych w systemie i forma tycznym lub papierowym.

....

Data podpis

ODWOŁANIE UPOWAŻNIENIA
DO PRZETWARZANIA DANYCH OSOBOWYCH
W PROGRAMIE.....

Z dniem .....r. odwołuję upoważnienie Pani/Panu .....do przetwarzania danych osobowych w systemie elektronicznym /papierowym w zbiorze/zbiorach .....programie Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej.

.....
Czytelny podpis Administratora Danych /osoby upoważnionej

WNIOSEK O NADANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH

Komórka organizacyjna.....

Proszę o nadanie upoważnienia do przetwarzania danych osobowych dla:

Pana/i.....pracownika komórki organizacyjnej.....realizującej zadania na podstawie umowy .....z dnia.....

w zbiorze/zbiorach:

.....

.....

.....

.....

data i podpis kierownika komórki organizacyjnej