Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze

Rozdział I
Przepisy ogólne, definicje i objaśnienia

§ 1

1. **Polityka Bezpieczeństwa** zwana dalej „Polityką" w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu danych osobowych przez Karkonoską Państwową Szkołę Wyższą w Jeleniej Górze dalej zwaną „Uczelnią". Przetwarzanie danych osobowych w Uczelni jest dopuszczalne tylko pod warunkiem przestrzegania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych, a także przepisów wewnętrznych wdrożonych na ich podstawie.
2. Celem Polityki jest:
   1) osiągnięcie i utrzymanie akceptowalnego poziomu bezpieczeństwa aktywów informacyjnych Uczelni poprzez wdrożenie odpowiedniego systemu ochrony tych aktywów przed zagrożeniami wewnętrznymi i zewnętrznymi,
   2) podniesienie poziomu świadomości pracowników Uczelni co do istoty problemu bezpieczeństwa danych osobowych.
3. Polityka ma zastosowanie do wszystkich postaci informacji zawierających dane osobowe: dokumentów papierowych, zapisów elektronicznych i innych, będących własnością Uczelni lub administrowanych przez Uczelnię i przetwarzanych w systemach informatycznych, tradycyjnych (papierowych) i komunikacyjnych Uczelni.
4. Ochrona danych osobowych wynikająca z Polityki jest realizowana na każdym etapie przetwarzania informacji.

§ 2

1. Dane osobowe w Uczelni przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
   1) Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z póź. zm.) zwana dalej „Ustawą",
   2) 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) – zwane dalej rozporządzeniem,
   3) art. 22 § 1-5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (j.t. Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) i przepisów wykonawczych wydanych z upoważnienia tej ustawy,
2. Dane osobowe w Uczelni przetwarzane są w zakresie realizacji jej statutowych, a w szczególności:
   1) dla zabezpieczania prawidłowego toku realizacji zadań dydaktycznych, naukowych, badawczych i organizacyjnych Uczelni wynikających z przepisów ustawy z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym. (Dz. U. z 2012 r. poz. 572 z późn. zm.),
   2) dla zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni, polityki personalnej oraz bieżącej obsługi stosunków pracy, studentów i innych osób wykonujących pracę na rzecz Uczelni,

3) dla realizacji innych usprawiedliwionych celów i zadań Uczelni - z poszanowaniem praw i wolności osób powierzających Uczelni swoje dane.

§ 3

Użyte w poniższych przepisach określenia oznaczają:
1. **Uczelnia** - Karkonoska Państwowa Szkoła Wyższa w Jeleniej Górze (KPSW).
2. **Ustawa** - ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. nr 101 poz. 926, z późn. zm.).
3. **Administrator danych osobowych (ADO)** – Rektor KPSW - decydujący, na podstawie art. 3 ustawy, o celach i środkach przetwarzania danych osobowych.
4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
5. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
6. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
7. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
8. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
9. **Administrator Bezpieczeństwa Informacji (ABI)**– osobę nadzorującą przestrzeganie zasad ochrony przetwarzania danych osobowych.
10. **Administrator Systemu Informatycznego (ASI)** – osobę odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach.
11. **Użytkownik** – osobę posiadającą pisemne zezwolenie wydane przez Rektora, dopuszczoną, w zakresie w nim wskazanym, do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej.
12. **Osoba trzecia** – każdą osobę bez zezwolenia do przetwarzania danych osobowych i przez to nieuprawnioną do dostępu do danych osobowych będących w posiadaniu administratora danych. Osobą trzecią jest również osoba posiadająca zezwolenie wydane przez Rektora, podejmująca czynności w zakresie przekraczającym ramy jej zezwolenia.

Rozdział II
Ogólne zasady przetwarzania danych osobowych

§ 4

1. Wszelkie dane osobowe gromadzone w Uczelni są przetwarzane na podstawie obowiązujących przepisów prawa, albo zgody osób fizycznych, których dane dotyczą lub na mocy umów z podmiotami zewnętrznymi (przetwarzane dane osobowe dotyczą głównie pracowników i studentów Uczelni).
2. Każda osoba, której dane osobowe znajdują się w posiadaniu Uczelni ma prawo przeglądać swoje dane oraz je modyfikować, w celu ich uzupełnienia lub poprawy.

3. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się **wysoki poziom bezpieczeństwa** przetwarzania danych osobowych w systemie informatycznym.
4. Wszelkie informacje zawierające dane osobowe są przechowywane w taki sposób, aby zminimalizować ryzyko ich ujawnienia, modyfikacji, zniszczenia lub utraty.
5. Dane osobowe są zabezpieczane fizycznie (np. przed awarią sprzętu), jak i elektronicznie (np. przed atakiem hakera lub dostępem niepowołanych osób).
6. Przetwarzanie danych osobowych w zakresie niezbędnym do wykonywania obowiązków służbowych powierza się wyłącznie na podstawie zaewidencjonowanych zezwoleń do przetwarzania danych osobowych.
7. W zakresie podmiotowym Polityka obowiązuje wszystkich pracowników Uczelni oraz inne osoby mające dostęp do danych osobowych.

Rozdział III
Organizacja ochrony przetwarzania danych osobowych

§ 5

1. Administratorem Danych Osobowych jest Rektor będący organem państwowej jednostki organizacyjnej, którą stanowi Uczelnia, realizujący obowiązki wynikające z Ustawy.
2. Obowiązki Administratora Danych Osobowych (ADO) wynikające z Ustawy w zakresie przetwarzania danych osobowych przez pracowników nie będących nauczycielami akademickimi, w imieniu Rektora, realizuje Kanclerz KPSW.
3. Obowiązki ADO wynikające z ustawy o ochronie danych osobowych wykonują, w imieniu Rektora, Lokalni Administratorzy Danych Osobowych, zwani dalej „LADO", to jest:
   1) prorektor - w zakresie podległych mu pracowników,
   2) dziekani wydziałów - w zakresie studentów wydziałów i podległych im pracowników,
   3) dyrektorzy/kierownicy pozostałych jednostek organizacyjnych – w zakresie podległych im pracowników.
4. Wykonanie obowiązków Lokalnego Administratora Danych Osobowych (LADO) następuje na podstawie upoważnienia stanowiącego załącznik nr 1.
5. Za naruszenie ustawy LADO ponoszą pełną odpowiedzialność w zakresie wnioskowanych zezwoleń względem podległych pracowników.
6. Funkcję Administratora Bezpieczeństwa Informacji (ABI), w Uczelni pełni osoba upoważniona przez Rektora.
   1) Głównymi zadaniami ABI są nadzór nad przeciwdziałaniem dostępowi osób nieuprawnionych do zbiorów danych oraz wykrywanie naruszeń w systemie ochrony i prawidłowego wykorzystywania danych osobowych.
   2) Powierzenie obowiązków ABI następuje na podstawie upoważnienia stanowiącego załącznik nr 9.
7. Obowiązki wynikające z ustawy o ochronie danych osobowych w zakresie zabezpieczenia systemów informatycznych sprawuje ABI za pośrednictwem Administratorów Systemów Informatycznych (ASI), których upoważnia Rektor.
8. Powierzenie obowiązków Administratora Systemu Informatycznego (ASI) następuje na podstawie upoważnienia stanowiącego załącznik nr 10.
9. Członek komisji Uczelnianej otrzymuje zezwolenie do przetwarzania danych osobowych, w zakresie umożliwiającym wykonywanie obowiązków członka komisji, na podstawie aktu prawa wewnętrznego, które jest źródłem jego powołania.

§ 6

Lokalni Administratorzy Danych Osobowych (LADO) zobowiązani są do przestrzegania

przepisów ustawy, w szczególności poprzez:

1) zapoznanie podległych pracowników z podstawowymi zasadami przetwarzania danych osobowych wynikającymi z ustawy, Polityki w zakresie ochrony danych osobowych w Uczelni, oraz Instrukcji Zarządzania Systemem Informatycznym w KPSW,
2) wykonywanie zaleceń Administratora Bezpieczeństwa Informacji (ABI) oraz Administratora Systemu Informatycznego (ASI) w zakresie ochrony danych osobowych,
3) bieżące przekazywanie do ABI wszelkich zmian mających wpływ na aktualizację ewidencji oraz praw dostępu do przetwarzania danych osobowych w systemach tradycyjnych,
4) bieżące przekazywanie do ASI wszelkich zmian mających wpływ na aktualizację ewidencji oraz praw dostępu do przetwarzania danych osobowych w systemach informatycznych,
5) współpracę z ASI, w zakresie wdrażania i nadzorowania przestrzegania Instrukcji Zarządzania Systemem Informatycznym,
6) występowanie z wnioskiem o nadanie uprawnień w systemie informatycznym oraz zezwoleń do przetwarzania danych osobowych podległym pracownikom; pracownika bez stosownego uprawnienia oraz zezwolenia LADO nie może dopuścić do przetwarzania danych osobowych,
7) informowanie ABI i Rektora o nieprawidłowościach w zakresie przetwarzania danych osobowych w systemach tradycyjnych.

§ 7

1. Administrator Bezpieczeństwa Informacji (ABI) realizuje zadania za pośrednictwem:
   1) pracowników Sekcji Kadr,
   2) Administratora Systemu Informatycznego (ASI).
2. Do zadań ABI należy ochrona danych osobowych przetwarzanych w Uczelni, a w szczególności:
   1) nadzór nad przestrzeganiem przez pracowników zasad ochrony danych osobowych obowiązujących w Uczelni,
   2) nadzór nad nadawaniem i odbieraniem uprawnień w systemie informatycznym oraz zezwoleń do przetwarzania danych osobowych, na wniosek osób upoważnionych oraz prowadzenie ewidencji uprawnień i zezwoleń,
   3) koordynacja procesu reagowania na naruszenia lub próby naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym oraz tradycyjnym,
   4) monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych osobowych oraz informowanie o nich Rektora,
   5) monitorowanie zaleceń i interpretacji Generalnego Inspektora Ochrony Danych Osobowych (GIODO) w zakresie ochrony danych osobowych,
   6) zgłaszanie do rejestracji zbioru danych osobowych do GIODO, na podstawie informacji otrzymanych od LADO.
3. Administrator Bezpieczeństwa Informacji (ABI) sprawuje nadzór nad realizacją zadań nałożonych na Lokalnych Administratorów Danych Osobowych (LADO) do przetwarzania danych osobowych.
4. Administrator Bezpieczeństwa Informacji (ABI) gromadzi i przechowuje dokumentację związaną z przetwarzaniem danych osobowych na terenie Uczelni.

§ 8

1. Pracownicy sekcji kadr KPSW zobowiązani są do :
   1) uzupełniania akt osobowych pracowników zatrudnionych przy przetwarzaniu danych

osobowych o oświadczenia, z których wynika, że zapoznali się z przepisami obowiązującymi w tym zakresie,

2) zgłaszania zmian kadrowych:

a) Administratorom Systemu Informatycznego (ASI) w celu aktualizacji praw dostępu do przetwarzania danych osobowych w systemach informatycznych,

b) Administratorowi Bezpieczeństwa Informacji (ABI) w celu aktualizacji ewidencji uprawnień do przetwarzania danych osobowych w systemach informatycznych

3) powiadamiania o dłuższej nieobecności w pracy ABI oraz ASI w celu niezwłocznego zawieszenia bądź wycofania uprawnień,

4) wykonywania, na polecenie Rektora, działań kontrolnych dotyczących przestrzegania przepisów w zakresie przetwarzania danych osobowych w systemach tradycyjnych.

2. Administrator Bezpieczeństwa Informacji (ABI) zobowiązany jest do wykonywania następujących obowiązków:

1) nadzorowania pracy Administratorów Systemu Informatycznego (ASI) w zakresie ochrony danych osobowych,

2) prowadzenia aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych,

3) organizacji szkolenia użytkowników w zakresie przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych,

4) wnioskowania do Działu Administracyjno-Technicznego o konieczne zakupy związane z ochroną danych osobowych,

5) wykonywania działań kontrolnych dotyczących przestrzegania przepisów w zakresie przetwarzania danych osobowych w systemach informatycznych,

6) zapewnienia zabezpieczenia systemów informatycznych zgodnie z wysokim poziomem bezpieczeństwa,

7) stosowania wszelkich dostępnych mechanizmów ochrony w celu właściwego zabezpieczenia systemu do przetwarzania danych,

8) zapewnienia ochrony danych osobowych poprzez tworzenie i właściwe zabezpieczenie kopii zapasowych,

9) zapewnienia prowadzenia w bezpieczny sposób napraw oraz konserwacji sprzętu i oprogramowania służącego do przetwarzania lub będącego nośnikiem danych osobowych,

10) zapewnienia niszczenia zbędnego sprzętu i oprogramowania zawierającego dane osobowe w sposób uniemożliwiający ich odczytanie,

11) informowania Rektora o nieprawidłowościach w zakresie przetwarzania danych osobowych.

12) wnioskowania do Lokalnych Administratorów Danych Osobowych (LADO), o przeprowadzenie kontroli dotyczącej przestrzegania Polityki w jednostkach organizacyjnych Uczelni.

§ 9

1. Administrator Bezpieczeństwa Informacji (ABI) prowadzi Rejestr zezwoleń/uprawnień (Użytkowników), zgodnie ze wzorem określonym w załączniku nr 2.

2. Udzielenie, modyfikacja, wycofanie zezwolenia/uprawnień odbywa się zgodnie z następującą procedurą:

1) Lokalny Administrator Danych Osobowych (LADO) występuje do Rektora z wnioskiem o udzielenie, zmianę lub wycofanie zezwolenia/uprawnień do przetwarzania danych osobowych (załącznik nr 3), który przekazuje do ABI.

2) w przypadku wnioskowania o uprawnienia do przetwarzania danych w systemie informatycznym, osoba określona we wniosku kierowana jest do ASI celem ustalenia

loginu do wnioskowanego systemu przetwarzania danych oraz odbycia szkolenia.
3) przed otrzymaniem zezwolenia do przetwarzania danych osobowych, pracownik bądź inna osoba zapoznaje się z obowiązującymi przepisami, a także przyjętymi w Uczelni zasadami bezpieczeństwa danych osobowych oraz zobowiązuje się do ich przestrzegania.
4) ABI na podstawie otrzymanego wniosku, któremu nadaje numer, wypełnia zezwolenie (załącznik nr 4), i w trzech egzemplarzach przekazuje do Rektora. Zaakceptowane i podpisane zezwolenie ABI wprowadza do rejestru nadając kolejny numer, z czego: jeden egzemplarz otrzymuje osoba, której udzielono zezwolenia, drugi egzemplarz jest przechowywany w aktach osobowych lub dokumentacji osoby, której udzielono zezwolenia, trzeci egzemplarz przechowuje ABI.
5) Zatwierdzony wniosek przechowuje i ewidencjonuje ABI.
6) nadanie, zmiana i wycofanie uprawnień odbywa się zgodnie z instrukcją zarządzania systemem informatycznym.

3. Upoważnienia i zezwolenia do przetwarzania danych osobowych wygasają z chwilą: ustania stosunku pracy, zmiany stanowiska lub zakresu obowiązków, a także z upływem okresu zezwolenia lub upoważnienia.
4. Każdy użytkownik posiadający zezwolenie do przetwarzania danych osobowych w systemie informatycznym otrzymuje od ASI jednoznaczny i niepowtarzalny login oraz stosowne uprawnienia w systemie.
5. Sposób uwierzytelnienia użytkownika w systemie informatycznym określa Instrukcja Zarządzania Systemem Informatycznym.
6. Użytkownicy zobowiązani są do:
1) ścisłego przestrzegania zakresu nadanego zezwolenia,
2) przetwarzania i ochrony danych osobowych zgodnie z przepisami,
3) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach),
4) zachowania w tajemnicy loginów i haseł uwierzytelniających użytkownika w systemie do przetwarzania danych osobowych,
5) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
6) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie,
7) niszczenia w sposób mechaniczny za pomocą niszczarek dokumentów, dokumentów zawierających dane osobowe po ustaniu ich przydatności jeśli nie są archiwizowane,
8) zgłaszania ASI i LADO zauważonych incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu, a także informowania ABI o przypadkach naruszenia zasad ochrony danych oraz o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe.
7. Pod szczególną ochroną przed niepowołanym dostępem do danych osobowych pozostają urządzenia wchodzące w skład systemu informatycznego Uczelni. W szczególności stacje robocze (poszczególne komputery) wchodzące w skład tego systemu, są umiejscawiane w sposób uniemożliwiający osobom nieuprawnionym, bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń służących do przetwarzania, a zwłaszcza kopiowania danych.
8. Dane osobowe przetwarzane w formach papierowych w sposób tradycyjny przechowuje się w sposób uniemożliwiający dostęp do nich osób bez zezwolenia, np. w zamkniętych szafach lub kasach pancernych.

Rozdział IV
Obszar przetwarzanych danych osobowych

§ 10

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w Uczelni jest prowadzony przez Administratora Bezpieczeństwa Informacji (ABI) na podstawie pisemnej informacji uzyskanej od Kanclerza. Wzór wykazu miejsc przetwarzania danych osobowych w Uczelni określa załącznik nr 5.

§ 11

1. Dostęp do budynków i pomieszczeń Uczelni, w których przetwarzane są dane osobowe podlega całodobowej kontroli dostępu.
2. Kontrola dostępu, o której mowa w ust. 1, polega na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się: nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia lub budynku oraz godzinę pobrania lub zdania klucza.
3. Klucze do budynków lub pomieszczeń, w których przetwarzane są dane osobowe wydawane mogą być wyłącznie pracownikom posiadającym zezwolenie do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych budynków, lub pomieszczeń na innych zasadach.
4. ABI przekazuje w formie pisemnej służbie ochrony budynku i aktualizuje wykaz pomieszczeń, do których dostęp jest ograniczony ze względu na przetwarzanie danych osobowych, zgodnie z § 10 oraz wykaz osób upoważnionych do pobierania kluczy do tych pomieszczeń, na podstawie informacji uzyskanych od LADO.
5. Opuszczenie pomieszczenia przez osobę przetwarzającą dane osobowe, wiąże się z zabezpieczeniem ich przed dostępem osób trzecich, z zastosowaniem dostępnych środków zabezpieczających.
6. Opuszczenie, noszące znamiona winy, przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne i jako takie traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

Rozdział V

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

§ 12

1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych oraz tradycyjnych, w zbiorach
ewidencyjnych oraz poza zbiorami.
2. W Uczelni przetwarzane są następujące zbiory danych:
   1) dane osobowe studentów,
   2) dane osobowe absolwentów,
   3) dane osobowe kandydatów na studia,
   4) dane osobowe pracowników,
   5) dane osobowe kandydatów do pracy,
   6) dane osobowe stażystów,
   7) dane osobowe byłych stażystów,
   8) dane osobowe byłych pracowników,
   9) dane osobowe osób, z którymi zawarto umowy cywilno-prawne,

10) dane osobowe osób, które posiadały umowy cywilno-prawne,
11) dane osobowe osób korzystających z Biblioteki,
12) dane osobowe osób, którzy korzystali z Biblioteki,
13) dane osobowe słuchaczy,
14) dane osobowe uczestników kursów,
15) dane osobowe byłych uczestników kursów,
16) dane osobowe osób korzystających z Domu Studenckiego,
17) dane osobowe osób, które korzystały z Domu Studenckiego.

3. Uczelnia posługuje się systemami informatycznymi wymienionymi w załączniku nr 6.

§ 13

1. Systemy informatyczne służące do przetwarzania danych osobowych zabezpieczone są przed działaniem niepożądanym przy pomocy odpowiednich form zabezpieczeń.
2. Dane osobowe w bazach danych umieszczonych na serwerach bazodanowych są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb komórek organizacyjnych Uczelni.

Rozdział VI
Opis struktury zbiorów danych osobowych wskazujących zawartość pól informacyjnych i powiązania między nimi

§ 14

1. Zawartość pól informacyjnych, występujących w aplikacjach (programach) systemów zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Rektora do przetwarzania danych osobowych.
2. Opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi wykonują ASI na podstawie aplikacji zastosowanych do przetwarzania tych danych, jeżeli opisów nie uzyskano od dostawców oprogramowania.
3. Opisy, o których mowa w ust. 2 mogą być wykonywane w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego ASI sporządzają inne dostępne opisy struktury zbioru.
4. ASI zobowiązani są do przekazywania opisów do ABI oraz niezwłocznego informowania o wszelkich zmianach w strukturze zbiorów danych, załącznik nr 7.

Rozdział VII
Sposób przepływu danych pomiędzy poszczególnymi systemami

§ 15

1. Schematy przepływu danych pomiędzy systemami informatycznymi, zastosowanymi w celu przetwarzania danych osobowych wykonują ASI, zgodnie z relacjami występującymi pomiędzy tymi systemami.
2. ASI zobowiązani są do przekazywania schematów przepływu danych pomiędzy systemami informatycznymi oraz niezwłocznego informowania o wszelkich zmianach do ABI.
3. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.

4. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (w szczególności dyskietki, płyty CD i DVD, dysku wymiennego, PenDrive'a) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji (w szczególności poprzez wewnętrzną sieć teleinformatyczną).
5. Wzór schematu przedstawiającego sposób przepływu danych osobowych pomiędzy poszczególnymi systemami określa załącznik nr 8.

Rozdział VIII
Opis zdarzeń naruszających ochronę danych osobowych

§ 16

1. Podział zagrożeń:
   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenie poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
      a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      b) nieuprawniony dostęp do systemu z jego wnętrza,
      c) nieuprawniony przekaz danych,
      d) pogorszenie jakości sprzętu i oprogramowania,
      e) bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana itp.;
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego,
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu,
   4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego, wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
   9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony danych osobowych albo inne strzeżone elementy systemu zabezpieczeń,

10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy stwierdzono naruszenie zabezpieczenia systemu informatycznego lub stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej wskazują na naruszenie zabezpieczeń tych danych.
4. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte w trakcie nieobecności w pomieszczeniu osoby upoważnionej szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), dyskietkach w formie niezabezpieczonej itp.

Rozdział IX
Zasady postępowania w sytuacji naruszenia ochrony danych osobowych

§ 17

1. Każdy Użytkownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym oraz w systemie tradycyjnym Uczelni zobowiązany jest do niezwłocznego poinformowania o tym Administratora Systemu Informatycznego (ASI), Lokalnego Administratora Danych Osobowych (LADO) lub w przypadku ich nieobecności Administratora Bezpieczeństwa Informacji (ABI).
2. ASI, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony bazy danych sytemu, którym administruje zobowiązany jest do niezwłocznego:
1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą, godziną i podpisania,
3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,
4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.: fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej, wylogowania użytkownika podejrzanego o naruszenie ochrony danych, zmianę hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu

uniknięcia ponownej próby uzyskania takiego dostępu,
5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą,
7) złożenie ABI raportu o zaistniałym wypadku naruszenia ochrony danych osobowych i podjętych krokach zabezpieczających.
8) przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości,
9) jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych,
10) jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości,
11) w porozumieniu z właściwym LADO przygotować szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia, przekazać do Rektora i ABI.

4. LADO w przypadku naruszenia ochrony danych osobowych w formie tradycyjnej (np. pozostawienia niezabezpieczonych przed dostępem osób postronnych dokumentów na: biurku, ksero lub drukarce, kradzieży dokumentów, niezamkniętej szafy, niewłaściwego zniszczenia dokumentów w sposób umożliwiający identyfikacje zawartych w nich danych osobowych, prace na danych osobowych w celach prywatnych itp.) ma obowiązek ponownie przeszkolić Użytkownika, a w przypadku zaniedbań sporządzić raport z zaistniałej sytuacji i poinformować o tym fakcie ABI.

5. Jeżeli przyczyną naruszenia zasad ochrony danych osobowych było zaniedbanie ze strony użytkownika systemu, Rektor może wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

Wzór dokumentu upoważnienia Lokalnego Administratora Danych Osobowych

Jelenia Góra, dnia ..... r.

UPOWAŻNIENIE LOKALNEGO ADMINISTRATORA DANYCH OSOBOWYCH

Nr .....[1]

Celem spełnienia wymogów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.):

upoważniam, Panią/Pana .....
(imię i nazwisko)

zatrudnioną(nego) na stanowisku/pełniącą(ego) funkcję .....

do pełnienia funkcji **Lokalnego Administratora Danych Osobowych** .....
(nazwa jednostki/komórki organizacyjnej)

.....

na okres .....

.....
(podpis Rektora)

.....
(podpis LADO)

[1] numer nadaje ABI

Wzór rejestru zezwoleń/uprawnień do przetwarzanie danych osobowych.

Lp.	Nazwisko	Imię	Komórka organizacyjna	Zakres uprawnień	Login	Numer zezwolenia	Data		Uwagi
							Nadania zezwolenia	Wycofania zezwolenia	

Jelenia Góra, dnia ..... r.

AKCEPTUJĘ:

.....
(Rektor/Kanclerz)

Wniosek
o (udzielenie/zmianę/wycofanie [1])
Zezwolenia
do przetwarzania danych osobowych

Nr.....[2]

dla Pani/Pana .....
(imię i nazwisko)

zatrudnionej/nego na stanowisku .....

w .....pomieszczenie ...../...../.....
(nazwa jednostki/komórki organizacyjnej) (obiekt/budynek/nr)

do przetwarzania danych osobowych, które obejmuje/obejmowało przetwarzanie

w zakresie .....

.....
(wymienić rodzaj danych)

w[3]..... login[4] : .....

na okres od ..... do .....

…..... .....
(podpis ASI) (podpis LADO)

[1] podkreślić właściwe
[2] numer nadaje ABI
[3] podać sposób przetwarzania danych np. w systemie informatycznym (podać nazwę systemu) lub/także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych (wymienić)
[4] (identyfikator użytkownika w systemie informatycznym) w przypadku nowego pracownika, po zatwierdzeniu Wniosku przez Rektora, login do systemu informatycznego zakłada ASI, w przypadku zmian login podaje osoba dla której składany jest wniosek

Jelenia Góra, dnia ..... r.

Zezwolenie
do przetwarzania danych osobowych
w Karkonoskiej Państwowej Szkole Wyższej
w Jeleniej Górze

nr .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm), Rektor/Kanclerz KPSW zezwalam
Pani/Panu:

.....
(imię i nazwisko)

.....
(nazwa jednostki/komórki organizacyjnej)

na przetwarzanie danych osobowych KPSW zgodnie z Wnioskiem nr .....

oraz zobowiązuje do przetwarzania danych osobowych zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi oraz obowiązującymi przepisami wewnętrznymi.

.....
(Rektor/Kanclerz)

.....
(data i podpis ABI)

.....
(data i podpis upoważnionego)

Zezwolenie wycofano dnia: .....

.....
(data i podpis ABI)

.....
(nazwisko i imię)

Jelenia Góra, dnia ..... r.

.....
(stanowisko służbowe oraz nazwa komórki organizacyjnej)

.....
(numer ewidencyjny)

OŚWIADCZENIE

Ja niżej podpisana/ny oświadczam, iż:

1. Zostałam/em przeszkolona/ny w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.) oraz Polityki Bezpieczeństwa w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze a także Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
2. Zobowiązuję się:
   - zachować w tajemnicy dane osobowe, z którymi zetknęłam się/zetknąłem się* w trakcie wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu;
   - chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.
3. Znana jest mi odpowiedzialność karna za naruszenie ustawy o której mowa w ust.1 (art. 49-54).

Przyjmuję do wiadomości, iż:

- sposoby zabezpieczenia danych osobowych stosowane w KPSW są tajemnicą Uczelni;
- postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez administratora danych osobowych 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, a także przepisów prawa cywilnego w przypadku umowy cywilno-prawnej.

.....
(podpis)

* niepotrzebne skreślić

Wzór wykazu miejsc przetwarzania danych osobowych w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze

Lp.	Nazwa zbioru danych[1]	Budynek	Nr pokoju[2]	Nazwa Systemu	Funkcja lokalizacji[3]	Zabezpieczenie fizyczne[4]

[1] nazwa zbioru danych osobowych zgodna z Polityką Bezpieczeństwa
[2] nazwa systemu do przetwarzania – tradycyjny (papierowy), informatyczny (nazwa systemu)
[3] S - serwer, K – miejsce przechowywania kopii bezpieczeństwa, Z – pomieszczenie, w którym wykonywane są kopie bezpieczeństwa,
U – pomieszczenie osób wprowadzających dane, A – pomieszczenie administratora bazy danych, P – pomieszczenie, gdzie przetwarza
się dane osobowe w sposób tradycyjny (papierowy), AP – archiwum zbiorów papierowych,
[4] A – alarm, W – wzmocnione drzwi

Dane aktualne na dzień.....

Sporządził.....

Wzór wykazu systemów informatycznych stosowanych do przetwarzania danych osobowych w KPSW

Lp.	Nazwa zbioru danych	Systemy informatyczne stosowane do przetwarzania danych osobowych w zbiorze	Zastosowany poziom bezpieczeństwa	Uwagi

Dane aktualne na dzień.....

Sporządził.....

Wzór struktury zbiorów danych

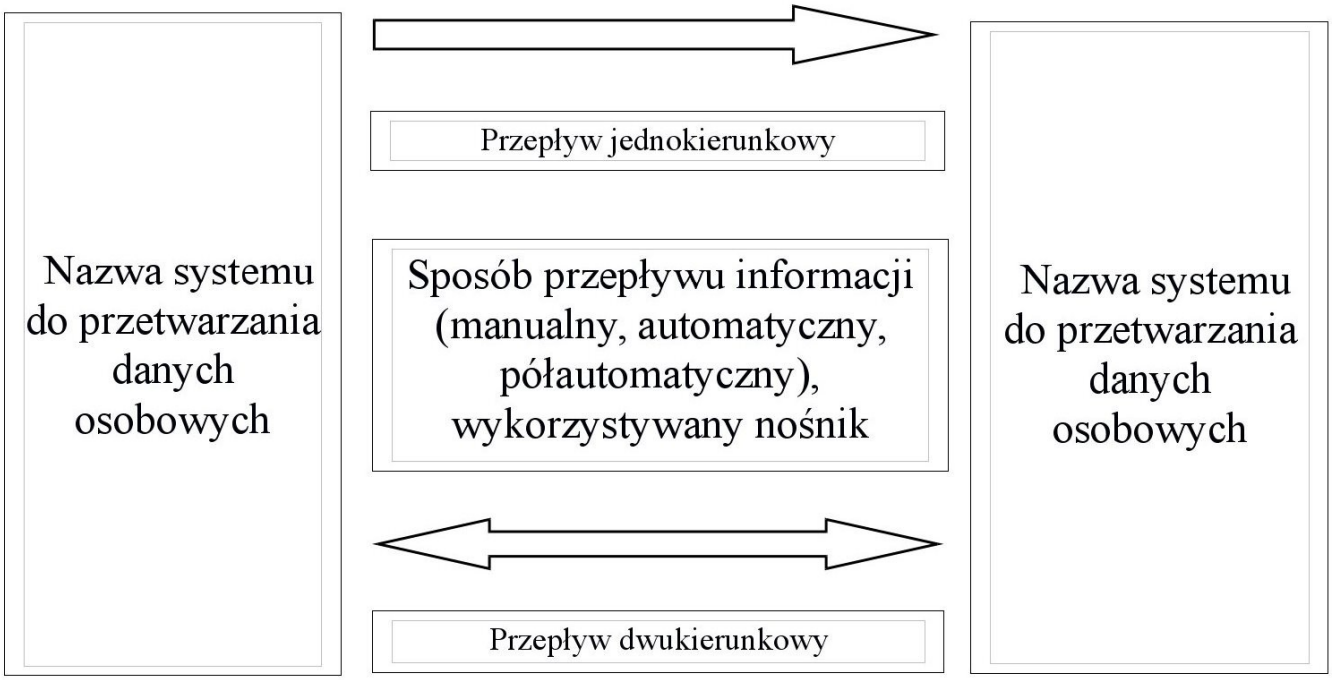
.....
System informatyczny stosowany do przetwarzania danych osobowych

Lp.	Nazwa zbioru danych	Zakres przetwarzanych danych

Dane aktualne na dzień.....

Sporządził.....

Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami.



Dane aktualne na dzień.....

Sporządził.....

..... Jelenia Góra dnia ..... r.
(pieczęć Uczelni)

UPOWAŻNIENIE
ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r., Nr 101, poz. 926 z późn. zm.)

z dniem .....

UPOWAŻNIAM

Panią/ Pana .....
(imię i nazwisko)

zatrudnioną/nego na stanowisku .....
(nazwa stanowiska, komórka organizacyjna)

do pełnienia funkcji

ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI
w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za bezpieczeństwa danych osobowych, w szczególności za przeciwdziałanie dostępowi osób niepowołanych do przetwarzanych danych osobowe oraz za podejmowanie działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

.....
(Rektor KPSW)

..... Jelenia Góra dnia ..... r.
(pieczęć Uczelni)

UPOWAŻNIENIE
ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

Na podstawie § 5.4 Polityki Bezpieczeństwa Danych Osobowych w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze, stanowiący Załącznik Nr 1 do Zarządzenia Nr ..... z dnia ..... Rektora Karkonoskiej Państwowej Szkoły Wyższej w Jeleniej Górze,

z dniem .....

UPOWAŻNIAM

Panią/ Pana .....
(imię i nazwisko)

zatrudnioną/nego na stanowisku .....
(nazwa stanowiska, komórka organizacyjna)

do pełnienia funkcji

ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

.....
(nazwa systemu informatycznego)

w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze

Administrator Systemu Informatycznego jest odpowiedzialny za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za prawidłowe funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków jego ochrony.

.....
(Rektor KPSW)