Załącznik nr 1
do Zarządzenia Rektora
nr R-0201-5/2019 z dnia 28 marca 2019 roku

POLITYKA BEZPIECZEŃSTWA
w zakresie ochrony danych osobowych
w Uniwersytecie Ekonomicznym w Krakowie

W ramach realizacji celów statutowych oraz innych celów wynikających z przepisów prawa Uniwersytet Ekonomiczny w Krakowie (dalej „Uczelnia" lub „UEK"), jako administrator danych osobowych stosuje politykę bezpieczeństwa w zakresie danych osobowych i spełnia wymagane prawem obowiązki wobec osób, których dane dotyczą.
Mając powyższe na uwadze ustala się następujące wytyczne polityki bezpieczeństwa danych osobowych w Uczelni, zwane dalej „Polityką bezpieczeństwa":

Rozdział I.
Postanowienia ogólne

§ 1

Przetwarzanie danych osobowych w Uczelni jest dopuszczalne pod warunkiem przestrzegania przepisów:

1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych praz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) – dalej RODO;
2) przepisów innych ustaw, a także rozporządzeń normujących problematykę przetwarzania danych osobowych;
3) wewnętrznych aktów normatywnych (uchwał Senatu UEK i zarządzeń Rektora) regulujących sprawy dotyczące ochrony danych osobowych.

§ 2

Uczelnia przetwarza dane osobowe:

1) w związku z realizacją zadań uczelni, wynikających z Ustawy z dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* (Dz.U. z 2018 r. poz. 1669, z późn.zm.),
2) w celu zapewnienia prawidłowej, zgodnej z prawem polityki personalnej oraz wypełnienia obowiązków prawnych ciążących na administratorze, jako pracodawcy,
3) dla realizacji innych celów i zadań – w szczególności wynikających z przepisów prawa lub prawnie uzasadnionych interesów administratora.

§ 3

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych, uwzględniając zasady wynikające z art. 5 RODO zapewnia, aby dane te były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości);
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89

ust. 1 RODO za niezgodne z pierwotnymi celami (zasada ograniczenia celu, celowości);
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości);
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą (zasada ograniczenia przechowywania);
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (zasada integralności i poufności);
7) przetwarzane w sposób, który pozwoli administratorowi wykazać, iż spełnione są zasady wymienione w pkt 1-6 (zasada rozliczalności).

2. Szczególnej ochronie podlegają dane osobowe wymienione w art. 9 ust.1 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, a także dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa – art. 10 RODO.

§ 4

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych odnosi się do danych osobowych przetwarzanych w:
   1) zbiorach danych tradycyjnych, na papierowych nośnikach danych (dokumentacja papierowa, np. kartoteki, księgi, wykazy, listy itp.),
   2) systemach informatycznych i na nośnikach cyfrowych,
   3) systemach dozoru wizyjnego (monitoring).
2. Polityka bezpieczeństwa w zakresie ochrony danych osobowych realizowana jest w Uniwersytecie Ekonomicznym w Krakowie przez wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, w szczególności przez osoby odpowiedzialne za nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z przepisów prawa oraz uregulowań wewnętrznych w tym zakresie, tj.:
   1) administratora danych osobowych (w osobie rektora) – **ADO** – zgodnie art. 24 RODO
   2) inspektora ochrony danych – **IOD** – zgodnie z art. 39 RODO
   3) inne osoby wykonujące zadania dotyczące przetwarzania i ochrony danych osobowych na podstawie udzielonych im upoważnień, w szczególności administratora systemów informatycznych - **ASI**.
3. Polityka bezpieczeństwa obowiązuje we wszystkich obiektach, lokalizacjach, komórkach organizacyjnych i stanowiskach pracowniczych Uczelni. Odnosi się do wszystkich chronionych danych osobowych przetwarzanych w Uczelni, niezależnie od formy, celu oraz zakresu ich przetwarzania (tradycyjnego i elektronicznego).
4. Procedury i zasady określone w Polityce bezpieczeństwa mają zastosowanie do wszystkich osób wykonujących prace związane z działalnością Uczelni lub na rzecz Uczelni (niezależnie od formy współpracy, czy rodzaju umowy) w szczególności pracowników, zleceniobiorców oraz osób realizujących umowy o dzieło.

5. UEK, jego pracownicy i współpracownicy deklarują pełne zaangażowanie dla bezpieczeństwa przetwarzania danych osobowych przetwarzanych zarówno w sposób tradycyjny, jak i w systemach informatycznych i na nośnikach cyfrowych.

§ 5

Uczelnia, jako administrator danych stosuje środki organizacyjne i techniczne, w tym informatyczne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, w szczególności wprowadza rozwiązania dotyczące:

1) pseudonimizacji i szyfrowania danych osobowych,
2) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych,
3) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, skutkującego naruszeniem ochrony danych osobowych,
4) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

§ 6

Dokumentacja dotycząca sposobu przetwarzania danych oraz środki ochrony danych osobowych powstają w oparciu o:

1) niniejszą Politykę bezpieczeństwa w zakresie ochrony danych osobowych,
2) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
3) inne wewnętrzne akty normatywne Uczelni, w tym zarządzenia Rektora, a także instrukcje, wytyczne i polecenia służbowe określające zasady i procedury dotyczące ochrony danych osobowych, wydawane przez upoważnione do tego osoby w poszczególnych jednostkach organizacyjnych.

Rozdział II.
Udostępnianie danych osobowych oraz prawa osób, których dane osobowe są przetwarzane w Uczelni

§ 7

Uczelnia, jako administrator danych udostępnia przetwarzane w swoich zasobach dane osobowe wyłącznie:

1) osobom, które przetwarzają dane osobowe na polecenie administratora tj. posiadającym upoważnienie do przetwarzania danych osobowych – co do zbioru i zakresu. Wzór upoważnienia znajduje się w Załączniku nr 1 do niniejszej Polityki. Upoważnienia wydawane są przez ADO po wcześniejszej akceptacji IOD. Upoważnienie może być cofnięte przed upływem okresu, na jaki zostało wydane – wzór cofnięcia upoważnienia znajduje się w załączniku nr 2. Wszystkie osoby, którym zostaje udzielone upoważnienie do przetwarzania danych osobowych są zobowiązane do podpisania oświadczenia o zachowaniu poufności danych osobowych zgodnie z załącznikiem nr 3.
2) podmiotom przetwarzającym, tj. osobom lub podmiotom, których charakter pracy wymaga udostępnienia im takich danych – na podstawie umowy powierzenia przetwarzania danych osobowych, która w szczególności określa:
   a) przedmiot i czas trwania przetwarzania
   b) charakter i cel przetwarzania
   c) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą
   d) obowiązki podmiotu przetwarzającego wynikające z art. 28 RODO

   Wzór umowy powierzenia przetwarzania danych osobowych stosowany w Uczelni stanowi załącznik nr 4 do niniejszej Polityki.

3) podmiotom kontrolnym uprawnionym do kontroli działalności administratora oraz podmiotom uprawnionym do przetwarzania danych osobowych – na podstawie przepisów prawa.

§ 8

Każda osoba, której dane osobowe dotyczą, na podstawie art. 15 RODO ma prawo do uzyskania potwierdzenia, czy jej dane osobowe są przetwarzane w Uczelni, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji o:

1) celu przetwarzania;
2) kategorii odnośnych danych osobowych;
3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) w miarę możliwości - planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
5) prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) prawie wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
8) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

§ 9

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia administratora danych osobowych lub upoważnionej przez niego osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa.
2. Dostęp do danych osobowych, o którym mowa w ust. 1, po okazaniu dokumentów potwierdzających uprawnienia mogą mieć w szczególności pracownicy: Państwowej Inspekcji Pracy, Zakładu Ubezpieczeń Społecznych, organów skarbowych, policji i służb specjalnych (Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego), sądów powszechnych, Najwyższej Izby Kontroli, Urzędu Ochrony Danych Osobowych, a także inne osoby, podmioty i organy upoważnione przez przepisy prawa i działające w granicach przyznanych im uprawnień.

Rozdział III.
Budynki, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe

§ 10

1. W Uczelni ewidencjonowane są budynki, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe. W budynkach tych i pomieszczeniach zastosowane są rozwiązania uniemożliwiające dostęp osób nieuprawnionych do zbiorów danych osobowych, w tym zabezpieczenia fizyczne, w szczególności wzmocnione drzwi, pomieszczenia zamykane na klucz, wejścia kodowane, elektroniczne systemy alarmowe, zamykane na klucz meble biurowe, zabezpieczenie okien (kraty i folia antywłamaniowa), alarm przeciwpożarowy, dozór z użyciem kamer.
2. Jeżeli dane osobowe przetwarzane są tylko w części pomieszczenia, pomieszczenie takie w miarę możliwości powinno być wyraźnie podzielone na:
   1) część ogólnodostępną,

2) część, w której przetwarzane są dane osobowe.
3. Wydzielenie części pomieszczenia może być w szczególności dokonane poprzez:
   1) montaż barierek lub lad,
   2) odpowiednie ustawienie mebli biurowych.
4. Pod szczególną ochroną pozostają urządzenia stanowiące zasoby sprzętowe systemu informatycznego – stacje robocze pracowników przetwarzających dane osobowe wchodzące w skład tego systemu powinny być umiejscowione w taki sposób, aby uniemożliwić dostęp osobom nieuprawnionym (w szczególności dostęp do monitorów oraz urządzeń służących do kopiowania danych).
5. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określają kierownicy jednostek organizacyjnych w których przetwarzane są dane osobowe - zgodnie z załącznikiem nr 5 do niniejszej Polityki bezpieczeństwa.
6. Wykaz budynków o których mowa w ust. 5 wymaga zatwierdzenia przez ADO.
7. Wykaz budynków o którym mowa w ust. 5 przechowuje IOD, a kopie wykazu - kierownicy jednostek organizacyjnych w których przetwarzane są dane osobowe
8. W budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu i / lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych.
9. Osoby nie upoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe - wyłącznie w obecności upoważnionego pracownika.

§ 11

1. Dostęp do budynków i pomieszczeń, w których przetwarzane są dane osobowe podlega nadzorowi i kontroli.
2. Nadzór, o którym mowa w ust. 1 dokonywany jest w danej jednostce organizacyjnej przez jej kierownika.
3. Kontrola, o której mowa w ust. 1 polega na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. Czynność tę wykonują osoby pracujące w portierniach. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia lub budynku oraz datę i godzinę pobrania lub zwrotu klucza.
4. Kierownik jednostki organizacyjnej, w której przetwarzane są dane osobowe pisemnie informuje portiera wydającego klucze o osobach upoważnionych do wejścia do pomieszczeń, w których przetwarzane są dane osobowe.
5. Klucze do budynków i / lub pomieszczeń, w których przetwarzane są dane osobowe mogą być wydawane wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym na innych zasadach do dostępu do tych budynków lub pomieszczeń.
6. Możliwe jest również wprowadzenie innej formy monitorowania dostępu do obszarów przetwarzania danych osobowych na przykład z użyciem kart elektronicznych i systemów jednoznacznie rejestrujących fakt użycia danej karty, a także z użyciem systemu dozoru wizyjnego. Pomieszczenia, w których przechowuje się duże ilości dokumentów zawierających dane osobowe (np. pomieszczenia Działu Spraw Pracowniczych) są dodatkowo zabezpieczone alarmem antywłamaniowym.
7. Szczegółowe zasady kontroli dostępu do poszczególnych obszarów (budynków, pomieszczeń) Uczelni, w których przetwarzane są dane osobowe określane są przez osoby kierujące poszczególnymi jednostkami organizacyjnymi Uczelni, w których takie

obszary występują. W przypadku nie określenia szczegółowych zasad kontroli stosuje się przepisy niniejszej Polityki.

§ 12

1. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe wiąże się z zastosowaniem wszystkich dostępnych środków zabezpieczających to pomieszczenie przed wejściem tam osób niepowołanych.
2. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, wiąże się z zastosowaniem dostępnych środków zabezpieczających, by chronić używane zbiory danych osobowych przed dostępem do nich osób nieuprawnionych.
3. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne, i będzie traktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

Rozdział IV.
Informacje dotyczące zbiorów danych osobowych

§ 13

1. Uczelnia sprawuje nadzór nad zbiorami danych osobowych tworzonymi na jej obszarze.
2. Zbiory, o których mowa w ust. 1 są uwzględnione w wykazie, który wymaga zatwierdzenia przez ADO. Wykaz zbiorów danych osobowych obejmuje nazwy zbiorów danych oraz wykaz programów / systemów informatycznych stosowanych do ich przetwarzania. Wzór wykazu stanowi załącznik nr 6 do niniejszej Polityki.
3. Wykazy o których mowa w ust. 2 opracowują kierownicy jednostek organizacyjnych, w których przetwarzane są dane osobowe dla zbiorów przetwarzanych wyłącznie w danej jednostce organizacyjnej, a w przypadku modułów systemów wykorzystywanych przez kilka jednostek, przez kierownika jednostki organizacyjnej będącej głównym użytkownikiem danego modułu.
4. Wykazy o których mowa w ust. 2 powinny być tworzone w postaci zgodnej z załącznikiem nr 6 – dopuszcza się inną postać tworzenia tych wykazów z zastrzeżeniem zawarcia w nich wszystkich wymaganych informacji.
5. Wykazy zbiorów danych przechowywane są przez IOD.
6. Wprowadzenie zmian funkcjonalnych w programach i systemach informatycznych przetwarzających dane osobowe wprowadzające zmiany w strukturze zbiorów danych wymaga opracowania nowych wykazów, o których mowa w ust. 2.
7. Wszelkie nowe programy i systemy informatyczne, które służyć mają gromadzeniu i przetwarzaniu danych osobowych muszą zapewniać zgodność z wymaganiami RODO, w szczególności muszą być dostarczone wraz z wykazami, o których mowa w ust. 2.
8. Decyzję o dopuszczeniu nowych programów lub systemów informatycznych, o których mowa w ust. 7 podejmuje IOD na wniosek kierownika jednostki organizacyjnej, w której mają zastosowanie nowe programy lub systemy informatyczne.
9. Uczelnia, jako administrator danych osobowych prowadzi rejestr czynności przetwarzania, zgodnie z art. 30 RODO. Rejestr uwzględnia zbiory danych z wykazów, o których mowa w ust. 2. Rejestr czynności przetwarzania danych osobowych jest aktualizowany na bieżąco, po każdej zmianie, o której mowa w ust. 6.
10. W przypadkach, gdy Uczelnia jest podmiotem przetwarzającym w rozumieniu art. 28 RODO, na mocy umowy powierzenia przetwarzania danych osobowych – prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.
11. Nadzór nad aktualizacją rejestrów, o których mowa w ust. 9-10 sprawuje IOD.

§ 14

W Uczelni zapewnia się ochronę zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z realizowaną dydaktyką. Zbiory te, po ich wykorzystaniu są niezwłocznie usuwane albo poddane modyfikacji tak, by danych w nich zawartych nie można było przypisać konkretnej lub dającej się ustalić osobie lub aby konieczny był w tym celu nieproporcjonalnie duży nakład czasu, kosztów i pracy (pseudonimizacja lub szyfrowanie).

§ 15

Zabronione jest przetwarzanie danych osobowych, w tym tworzenie zbiorów takich danych, a także gromadzenie w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne dla realizacji celów, do których dane te zostały zebrane.

Rozdział V.
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

§ 16

Zasady ogólne dotyczące bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych:

1) dane osobowe w systemach informatycznych przetwarzać może wyłącznie osoba posiadająca pisemne upoważnienie. Pracownicy / współpracownicy mają dostęp wyłącznie do takich informacji i danych jakie się wiążą z wykonywaną przez nich pracą, której zakres został określony w umowie o pracę lub umowie cywilnoprawnej oraz
   w zakresie zadań / obowiązków (zasada wiedzy koniecznej);
2) dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest
   w sposób jednoznaczny przypisany użytkownikowi, który jest odpowiedzialny za wszystkie czynności wykonywane przy jego użyciu. Pracownik może przetwarzać dane osobowe tylko w zakresie wskazanym w nadanym przez pracodawcę upoważnieniu do przetwarzania danych osobowych;
3) rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

§ 17

W Uczelni zapewnione są środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, w szczególności:

1) prowadzona jest polityka bezpieczeństwa w zakresie ochrony danych osobowych, która w miarę potrzeby jest na bieżąco aktualizowana;
2) wprowadzona jest *Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji w Uniwersytecie Ekonomicznym w Krakowie*;
3) wprowadzona jest *Instrukcja zarządzania system informatycznym służącym do przetwarzania danych osobowych*;
4) prowadzone są szkolenia wewnętrzne i wydawane są instrukcje oraz zalecenia podnoszące świadomość pracowników w zakresie bezpieczeństwa przetwarzania danych osobowych;

5) promowana jest ogólna zasada poufności danych osobowych – w każdym aspekcie funkcjonowania Uczelni;
6) wprowadzona jest *Polityka czystego biurka*, zgodnie z załącznikiem nr 7 do niniejszej Polityki;
7) powołany jest Inspektor Ochrony Danych (IOD);
8) prowadzona jest ocena ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w związku z przetwarzaniem danych osobowych;
9) dokonywana jest ocena skutków dla ochrony danych osobowych w odniesieniu do planowanych operacji przetwarzania, w szczególności z użyciem nowych technologii – w przypadku, gdy zostanie stwierdzone, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
10) prowadzona jest ewidencja osób, którym nadano upoważnienie do przetwarzania danych osobowych;
11) prowadzona jest kontrola dostępu do pomieszczeń, w których przetwarzane są dane osobowe oraz ścisła kontrola dostępu do pomieszczeń, w których znajdują się serwery
12) prowadzona jest sprzętowa i programowa ochrona danych na serwerach i stacjach roboczych, z pomocą których przetwarzane są dane osobowe, w tym:
    a) tworzenie kopii zapasowych baz danych zawierających dane osobowe,
    b) ograniczenie ruchu dla usług publicznych i jego ochrona przy pomocy access-list na routerach i udostępnianie tylko wybranych portów na serwerach,
    c) stosowanie zapory ogniowej - firewall oraz jej bieżący monitoring,
    d) stosowanie ochrony antywirusowej,
    e) zezwolenie na przetwarzanie danych osobowych stanowiących zasoby Uczelni przy użyciu komputerów przenośnych – wyłącznie w przypadkach, gdy komputery takie stanowią wyposażenie pracowników (sprzęt służbowy) i są odpowiednio zabezpieczone (zaszyfrowane);
    f) zezwolenie na przetwarzanie, w szczególności przechowywanie danych osobowych stanowiących zasoby Uczelni na nośnikach cyfrowych (dysk przenośny, pendrive itp.) – wyłącznie w przypadkach, gdy nośniki takie stanowią wyposażenia pracowników (sprzęt służbowy) i są odpowiednio zabezpieczone (zaszyfrowane);
    g) wprowadzony jest zakaz przetwarzania danych osobowych, które nie stanowią zasobów Uczelni (dane prywatne) na służbowym sprzęcie.

Rozdział VI.
Postanowienia końcowe

§18

1. Uczelnia na bieżąco dokłada wszelkich starań, aby gromadzone i przetwarzane dane osobowe podlegały ochronie zgodnie z wymogami obowiązującego w tym zakresie prawa.
2. Mając na uwadze stałe podnoszenie poziomu bezpieczeństwa przetwarzania danych osobowych, Uczelnia wdraża środki techniczne (w tym informatyczne) i organizacyjne, które pozwalają minimalizować ryzyko związane z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Polityka bezpieczeństwa powinna być poddana analizie przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych IOD może zarządzić analizę polityki bezpieczeństwa stosownie do potrzeb. IOD analizuje, czy polityka bezpieczeństwa jest adekwatna do zmian:
    a) organizacyjnych w Uczelni, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,

b) w obowiązującym prawie.

4. Wraz z przeglądem Polityki bezpieczeństwa IOD kontroluje również pracowników i inne podmioty upoważnione do przetwarzania danych osobowych pod kątem przestrzegania przez te osoby niniejszej Polityki, Instrukcji Zarządzania System Informatycznym oraz przepisów RODO (audyty doraźne).
5. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie potwierdzające znajomość jego treści.

Załączniki:

- Zał. 1 – wzór upoważnienia do przetwarzania danych osobowych;
- Zał. 2 – wzór cofnięcia upoważnienia;
- Zał. 3 – wzór oświadczenia o zachowaniu poufności;
- Zał. 4 – wzór umowy powierzenia przetwarzania danych osobowych;
- Zał. 5 – wzór wykazu budynków i pomieszczeń, w których przetwarzane są dane osobowe;
- Zał. 6 – wzór wykazu zbiorów danych i programów/systemów informatycznych
- Zał. 7 - Polityka czystego biurka