Załącznik nr 2
do Zarządzenia Rektora
nr R-0201-5/2019 z dnia 28 marca 2019 roku.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie Ekonomicznym w Krakowie

1. Ilekroć w niniejszej instrukcji jest mowa o:
   1) RODO – należy przez to rozumieć Rozporządzenie 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 rozporządzenie o ochronie danych osobowych)
   2) ADO – administrator danych osobowych,
   3) IOD – inspektor ochrony danych,
   4) ASI – administrator systemu informatycznego – rozumie się przez to osobę posiadającą uprawnienia do zarządzania zasobami sieci i systemów informatycznych (całymi lub wydzielonymi)
   5) ADM – osoba uprawniona do wykonywania prac administracyjnych w systemie informatycznym (tzw. „admin”),
   6) Kierownik – dyrektor lub kierownik jednostki organizacyjnej, w której przetwarzane są dane osobowe.
2. Do zabezpieczenia danych osobowych przetwarzanych w Uczelni stosuje się zasady i środki określone w *Polityce bezpieczeństwa w zakresie danych osobowych w Uniwersytecie Ekonomicznym w Krakowie* oraz w niniejszej *Instrukcji*.

Rozdział I.
Osoby przetwarzające dane osobowe

1. Realizując *Politykę bezpieczeństwa w zakresie ochrony danych osobowych w Uniwersytecie Ekonomicznym w Krakowie* wyznacza się osoby odpowiedzialne za bieżącą realizację tej polityki na terenie Uczelni oraz w jej poszczególnych jednostkach organizacyjnych. Za realizację polityki bezpieczeństwa odpowiadają w szczególności:
   1) rektor - jako administrator danych osobowych (ADO) w rozumieniu art. 24 RODO,
   2) inspektor ochrony danych (IOD) w rozumieniu art. 37 RODO – w zakresie bieżącej analizy Polityki i jej aktualizacji oraz kontroli jej przestrzegania (audyty doraźne),
   3) administrator systemu informatycznego (ASI) – w zakresie bieżącego nadzoru nad stosowaniem procedur związanych zarządzaniem systemem informatycznym oraz jego użytkowaniem przy zachowaniu wymogów bezpieczeństwa,
   4) inne osoby mające dostęp do danych osobowych w systemach informatycznych zgodnie z upoważnieniem udzielonym przez administratora.
2. Osoby upoważnione do przetwarzania danych osobowych zostają zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą. W szczególności są one informowane o obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia i składają w tym zakresie stosowne oświadczenie na piśmie.
3. W przypadku naruszenia zasad bezpiecznego i zgodnego z prawem przetwarzania danych osobowych przez osoby zatrudnione w ramach stosunku pracy upoważnione

do przetwarzania takich danych, działanie takie traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.

Rozdział II.
Nadawanie uprawnień do przetwarzania danych w systemie informatycznym i rejestrowanie tych uprawnień oraz wskazanie osoby odpowiedzialnej za te czynności

1. Dane osobowe w systemach informatycznych może przetwarzać wyłącznie osoba posiadająca stosowne upoważnienie do przetwarzania danych osobowych udzielone przez ADO na postawie wniosku kierownika jednostki organizacyjnej Uczelni.
2. IOD prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych w Uczelni. Upoważnienia do przetwarzania danych osobowych są przechowywane w aktach osobowych pracowników.
3. Na wiosek kierownika jednostki organizacyjnej Uczelni upoważnienie do przetwarzania danych osobowych może zostać cofnięte przed terminem jego wygaśnięcia. Kierownik jednostki organizacyjnej Uczelni powinien o tym fakcie pisemnie poinformować zainteresowanego.
4. Fakt cofnięcia upoważnień do przetwarzania danych osobowych jest odnotowywany w rejestrze, o którym mowa w ust. 2.
5. Osoby upoważnione do przetwarzania danych osobowych gromadzonych w zasobach sieci administracyjnej posiadają indywidualne konto. Sposób rejestrowania kont reguluje obowiązujący w Uczelni odrębny Regulamin sieci administracyjnej LAN.

Rozdział III.
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie użytkownik po podaniu identyfikatora i właściwego hasła.
2. Identyfikator (login) jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.
3. Sposób tworzenia identyfikatora - loginu i hasła - opisany jest w załączniku nr 1 do Regulaminu sieci LAN-ADM, o którym mowa w Rozdz. II ust. 5 niniejszej Instrukcji.
4. System informatyczny, w którym przetwarzane są dane osobowe jest skonfigurowany w sposób wymagający bezpiecznego zarządzania hasłami użytkowników:
    1) pierwsze hasło użytkownik określa samodzielnie, w sposób zgodny z załącznikiem 1 do regulaminu LAN-ADM, o którym mowa w Rozdz. II ust. 5 niniejszej Instrukcji;
    2) hasło, o którym mowa w pkt 1 musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego,
    3) kolejne hasła są zmieniane przez użytkownika,
    4) system informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła w ustalonych odstępach czasu, nie dłuższych niż 30 dni od dnia ostatniej zmiany hasła,
    5) system informatyczny wyposażony jest w mechanizmy pozwalające na wymuszenie jakości hasła, w szczególności hasło powinno składać się z co najmniej 8 znaków - powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
    6) hasła dostępu do systemu tworzone są przez użytkownika i stanowią tajemnicę znaną wyłącznie temu użytkownikowi,

7) użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie,
8) hasła nie są zapisywane w systemie informatycznym w postaci jawnej,
9) hasła nie mogą być przechowywane przez użytkowników w formie jawnej w żadnej postaci elektronicznej lub tradycyjnej, w szczególności w miejscach, gdzie może dojść do nieautoryzowanego dostępu ze strony osób trzecich.

5. Na potrzeby administrowania systemem tworzone są uniwersalne konta administracyjne typu „admin”.
6. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne, do których mają przydzielone hasło. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników.
7. Identyfikatory i hasła kont administracyjnych typu ”admin” są przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie dyrektor Centrum Informatyki oraz jego zastępcy. Identyfikatory oraz hasła osób uprawnionych do wykonywania prac administracyjnych oraz użytkowników są przechowywane w oznakowanej i podpisanej kopercie.
8. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczne jest udokumentowanie zaistniałej sytuacji poprze dokonanie wpisu w „Dzienniku haseł”, który znajduje się w tej samej szafie, w której znajduje się koperta z hasłami użytkowników. Nadzór nad „Dziennikiem haseł” sprawuje dyrektor Centrum Informatyki lub jego zastępcy.
9. Wpis, o którym mowa w ust.8, powinien zawierać następujące informacje:
   1) imię i nazwisko oraz stanowisko osoby upoważnionej umożliwiającej dostęp do szafy, w której znajdują się hasła,
   2) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
   3) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

Rozdział IV.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Przed rozpoczęciem oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia szczególnej uwagi, czy nie wystąpiły przesłanki mogące świadczyć o naruszeniu ochrony danych osobowych.
2. O naruszeniu ochrony danych osobowych mogą świadczyć następujące przesłanki:
   1) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
   2) brak możliwości zalogowania się do tej aplikacji,
   3) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
   4) wygląd aplikacji inny niż normalnie,
   5) inny zakres danych niż normalnie dostępny dla użytkownika,
   6) znaczne spowolnienie działania systemu informatycznego,
   7) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
   8) ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
   9) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych,

10) włamanie lub próby włamania do szafek, w których przechowywane są – w postaci elektronicznej lub papierowej – nośniki danych osobowych,
11) zagubienie bądź kradzież nośnika danych osobowych,
12) zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, dyskietki itp.),
13) kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
14) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
15) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,
16) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

3. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
4. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych
na poziomie danego użytkownika.
5. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z kierownikiem jednostki. Konieczność odblokowania konta jest zgłaszana administratorowi systemu informatycznego w formie pisemnej.
6. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut, automatycznie włączany jest program do wygaszania ekranu. Programy do wygaszania ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.
7. Hasło o którym mowa w ust. 6 powyżej powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
8. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika.
9. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólnie jedno konto użytkownika.
10. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut, użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe.
11. W pomieszczeniach, w których przetwarzane są dane osobowe i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
12. Prawidłowe zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

Rozdział V.
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za proces tworzenia kopii zapasowych na serwerach odpowiada osoba uprawniona do wykonywania prac administracyjnych w systemie informatycznym (ADM).

3. Kopie zapasowe na serwerach wykonywane są codziennie w godzinach nocnych, na zewnętrzne nośniki danych, inne niż te służące do ich bezpośredniego przetwarzania. Do przechowywania kopii zapasowych służą:
   1) serwery kopii – dane oraz programy służące do ich przetwarzania są kopiowane codziennie i są przechowywane przez okres 60 dni od daty ich wykonania. Kopiowanie danych przebiega z wykorzystaniem sieci teleinformatycznej odseparowanej od sieci publicznej. Dostęp do serwera chroniony jest poprzez system identyfikatorów i haseł, oraz poprzez nadawanie użytkownikom odpowiednich uprawnień do sporządzania, odczytu oraz odtwarzania kopii zapasowych. Fizyczny dostęp do serwerów zabezpieczony jest poprzez umiejscowienie ich w pomieszczeniach nie posiadających okien, oraz poprzez system alarmowy. Serwery umieszczone są w innym budynku niż serwery na których przetwarzane są dane osobowe. Dostęp do pomieszczenia posiadają tylko wybrani administratorzy.
   2) zewnętrzne streamery - archiwizacja przebiega codziennie, dane są kopiowane przy wykorzystaniu programu specjalistycznego, który zainstalowany jest na serwerze kopii. Urządzenie zainstalowane jest w tym samym pomieszczeniu, co serwer kopii. Dostęp fizyczny do urządzenia zabezpieczony jest identycznie jak w przypadku serwerów kopii.
4. W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator LAN-ADM.
5. Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, są pozbawiane zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W braku takiej możliwości nośniki podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

Rozdział VI.
Sposób, miejsce i okres przechowywania nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem.
2. Dane osobowe przetwarzane w programach i systemach informatycznych nie mogą być zapisywane na nośnikach przenośnych, które nie są odpowiednio zabezpieczone (zaszyfrowane) i nie mogą być wykorzystywane do tworzenia kopii zapasowych.
3. Ewentualne wydruki (dane w postaci papierowej) powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar.
4. W przypadku, gdy nośnik danych osobowych nie jest już potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika - tak, by danych tych nie można było przypisać konkretnej lub dającej się ustalić osobie.
5. Jeżeli wydruk danych osobowych nie jest już potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

Rozdział VII.
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem

jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W celu przeciwdziałania oprogramowaniom, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego wprowadzone są następujące zabezpieczenia:
   1) odseparowanie serwerów bazy danych od sieci zewnętrznej,
   2) autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
   3) stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
   4) stosowanie aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
   5) stosowanie szyfrowanej transmisji danych,
   6) stosowanie odpowiedniej ochrony antywirusowej i ochrony zapór ogniowych na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych,
   7) stosowanie wyłącznie licencjonowanego oprogramowania.
2. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
   1) załączniki do poczty elektronicznej,
   2) przeglądane strony internetowe,
   3) pliki i aplikacje pochodzące z niezabezpieczonych nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.
3. W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego przetwarzającego dane osobowe, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:
   1) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
   2) antywirusowy skaner ruchu internetowego powinien być stale włączony,
   3) monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony,
   4) skaner poczty elektronicznej powinien być stale włączony.
4. Systemy antywirusowe zainstalowane na stacjach roboczych skonfigurowane są w sposób uniemożliwiający ingerencję użytkownika w ustawienia oprogramowania. System zapewnia centralne uaktualnienia wzorców wirusów.
5. System antywirusowy jest aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.
6. Użytkownicy systemu informatycznego zobowiązani są do następujących działań:
   1) skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – na bieżąco,
   2) skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
   3) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.
7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
   1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
   2) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

8. W systemie informatycznym może być eksploatowane wyłącznie legalne oprogramowanie, instalowane wyłącznie przez uprawnionych administratorów.

Rozdział VIII.
Wymogi, jakie spełnia system informatyczny służący do przetwarzania danych osobowych

1. System informatyczny służący do przetwarzania danych osobowych posiada mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika
   do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).
2. System informatyczny służący o przetwarzania danych osobowych musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych:
   1) data pierwszego wprowadzenia danych osobowych do zbioru,
   2) identyfikator osoby wprowadzającej te dane,
   3) źródło danych (w przypadku pozyskania ich nie od osoby, której te dane dotyczą),
   4) informacja o udostępnieniu danych osobowych,
   5) sprzeciw dotyczący przetwarzania danych osobowych,
   6) sporządzania i wydrukowania raportu.
3. Odnotowanie informacji, o których mowa w ust.2 pkt 1 i 2 odbywa się automatycznie, po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
4. System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
5. Zabezpieczenia systemu informatycznego są na bieżąco monitorowane przez administratora systemu informatycznego (ASI).

Rozdział IX.
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. Prace serwisowe są wykonywane wyłącznie przez pracowników Centrum Informatyki lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie pracowników Centrum Informatyki.
3. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
   3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej.
4. Wszelkie przeglądy i konserwacje stacji roboczych wykonywane są na bieżąco po wcześniejszym zgłoszeniu upoważnionemu pracownikowi Centrum Informatyki.

5. Przeglądy i konserwacje serwerów wykonywane są w ustalonych cyklach, wyłącznie przez osoby upoważnione.
6. Monitorowanie stanu pracy serwerów, w tym stanu dysków wykonywane jest w sposób ciągły przez administratorów systemu.
7. W przypadku konieczności wyłączenia serwera na przewidywany okres dłuższy niż 1 godzina użytkownicy powiadamiani są z dwudniowym wyprzedzeniem.

Rozdział X.
Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Naruszeniem zabezpieczenia systemu informatycznego przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną lub jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   1) nieautoryzowany dostęp do danych,
   2) nielegalne ujawnienie danych,
   3) pozyskiwanie danych z nielegalnych źródeł.
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie bezpieczeństwa przetwarzania danych osobowych, każdy pracownik zaangażowany w proces przetwarzania danych osobowych w Uczelni jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie poinformować o zaistniałej sytuacji przełożonego oraz Inspektora Ochrony Danych a następnie postępować stosownie do podjętej przez powiadomioną osobę decyzji.
3. W przypadku incydentu naruszenia ochrony danych osobowych, o którym mowa w ust. 2 obowiązują zasady określone w odrębnym Zarządzeniu Rektora w sprawie *Procedury zarządzania incydentami związanymi z bezpieczeństwem informacji w Uniwersytecie Ekonomicznym w Krakowie*.

Rozdział XI.
Postanowienia końcowe

1. Wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych (w tym przetwarzanie w systemie informatycznym) w Uczelni, bez względu na zajmowane stanowisko i miejsce wykonywania pracy oraz charakter stosunku pracy, są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej Instrukcji.
2. Nieprzestrzeganie zasad postępowania określonych w niniejszej Instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną zastosowania odpowiednich sankcji wynikających odpowiednio z odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy albo odpowiedzialności odszkodowawczej określonej w Kodeksie cywilnym.
3. Jeżeli skutkiem działania osoby upoważnionej do przetwarzania danych osobowych stanowiących zasoby Uczelni jest ujawnienie danych osobie nieuprawnionej lub sprzeczne z prawem ich wykorzystanie, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z Kodeksu Karnego.
4. Osoba, która przetwarza dane osobowe, choć ich przetwarzanie jest niedopuszczalne albo do ich przetwarzania nie jest uprawniona, może podlegać odpowiedzialności karnej wynikającej z ustawy o ochronie danych osobowych.

5. Jeżeli skutkiem działania lub zaniechania osoby upoważnionej do przetwarzania danych osobowych stanowiących zasoby Uczelni jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego i innych przepisów szczególnych znajdujących zastosowanie.
6. ADO zapewnia środki organizacyjne, techniczne i finansowe na realizację zadań wynikających z niniejszej instrukcji.