Załącznik nr 1 do Zarządzenia

Polityka bezpieczeństwa

Podstawy prawne i definicje:
- Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- Rozporządzenie - rozporządzenie 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
- Zarządzenie – zarządzenie nr 0121-20/2003 rektora Akademii Ekonomicznej w Krakowie w sprawie ochrony danych osobowych

Polityka bezpieczeństwa zgodnie z rozporządzeniem zawiera w szczególności
- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
- sposobu przepływu danych pomiędzy poszczególnymi systemami
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności integralności i rozliczalności przetwarzanych danych.

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych stanowi załącznik nr 1 dokumentu.
Dokument ten powinien być aktualizowany po zmianach lokalowych w odniesieniu do jednostek organizacyjnych, których pracownicy przetwarzają dane osobowe.
Aktualizacja następuje na wniosek właściwego lokalnego administratora danych osobowych.
Aktualny dokument przechowuje administrator danych.

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych znajduje się w Załączniku 2 do niniejszego dokumentu.
Dokument ten powinien być aktualizowany po wprowadzeniu do przetwarzania nowych zbiorów danych osobowych lub nowych programów, które je obsługują.
Aktualizacji dokonuje administrator danych osobowych we współpracy z administratorem sieci komputerowej. Aktualny dokument przechowuje administrator bezpieczeństwa informacji.

3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól i powiązania miedzy nimi
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduje się w załączniku 3 do niniejszego dokumentu.
Każdy załącznik powinien być aktualizowany po wprowadzeniu istotnych zmian w strukturze bazy danych, którą opisuje.
Aktualizacji dokonuje administrator danych osobowych we współpracy z administratorem sieci komputerowej. Aktualny dokument przechowuje administrator bezpieczeństwa informacji.

4. Sposób przepływu danych pomiędzy poszczególnymi systemami
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduje się w załączniku 4 do niniejszego dokumentu.
Dokument powinien być aktualizowany po wprowadzeniu istotnych zmian w sposobie lub zakresie wymiany danych, którą opisuje.
Aktualizacji dokonuje administrator danych osobowych we współpracy z administratorem sieci komputerowej. Aktualny dokument przechowuje administrator bezpieczeństwa informacji.

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
Zastosowane środki techniczne i organizacyjne stosowane dla zapewnienia poufności, integralności i rozliczności przetwarzanych danych obejmuje:
a) system nadawania uprawnień:
• dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
• identyfikator (login) jest w sposób jednoznaczny przypisany jednemu użytkownikowi
• 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.
b) kontrola dostępu i ochrona pomieszczeń w tym:
• wydawanie kluczy do pomieszczeń w których przebywają osoby przetwarzające dane osobowa na podstawie list
• ochrona pomieszczeń z użyciem elektronicznych alarmów antywłamaniowych
• wyposażenie pomieszczeń w których znajdują się serwery w system instalacji sygnalizującej pożar
• wyposażenie okien pomieszczeń w których znajdują się serwery w folie antywłamaniowe
c) zabezpieczenia sprzętowe i programowe w celu ochrony danych na stacjach roboczych i serwerach
• tworzenie kopii zapasowych baz danych zawierających dane osobowe
• ograniczenie ruchu dla usług publicznych i jego ochrona przy pomocy access-list na routerach i udostępnianie tylko wybranych portów na serwerach
• stosowanie zapory ogniowej - firewall oraz jej bieżący monitoring
• stosowanie ochrony antywirusowej
• nie dopuszczanie do przetwarzania danych osobowych z użyciem komputerów przenośnych

Załączniki do Polityki bezpieczeństwa

Załącznik 1
Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. – wzór dokumentu

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe			
LP	Lokalizacja	Nazwa budynku	Numery pomieszczeń

Załącznik 2
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych – wzór dokumentu

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
LP	Zbiór danych	Nazwa programu

Załącznik 3
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól i powiązania między nimi – wzór dokumentu

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól i powiązania między nimi				
Nazwa zbioru:				
LP	Nazwa pola	typ	długość	Opis

Załącznik 4
Sposób przepływu danych pomiędzy poszczególnymi systemami – wzór dokumentu

Sposób przepływu danych pomiędzy poszczególnymi systemami			
LP	Nazwa systemu	Nazwa systemu	Przepływ danych

Załącznik nr 2 do Zarządzenia

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Podstawy prawne i definicje:
- Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- Rozporządzenie - rozporządzenie 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
- Zarządzenie – zarządzenie nr 0121-20/2003 Rektora Akademii Ekonomicznej w Krakowie w sprawie ochrony danych osobowych

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności:

Administrator danych wystawia osobie przetwarzającej dane osobowe upoważnienie do przetwarzania danych osobowych zgodnie z załącznikiem 1. Administrator danych prowadzi rejestr wydanych upoważnień.
Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba będąca zarejestrowanym użytkownikiem sieci komputerowej posiadającym osobiste konto.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem:

Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
Identyfikator (login) jest w sposób jednoznaczny przypisany użytkownikowi i jest unikalny w systemie. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników:
- hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego,
- hasła są zmieniane przez użytkownika,
- system informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła w odstępach nie dłuższych niż 8 dni od dnia ostatniej zmiany hasła,
- system informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła, w szczególności hasło powinno składać z co najmniej 8 znaków. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
- hasła dostępu do systemu tworzone są przez użytkownika i stanowią tajemnicę znaną wyłącznie temu użytkownikowi,

- użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie,
- hasła nie mogą być przechowywane w formie jawnej w żadnej postaci elektronicznej lub tradycyjnej szczególnie w miejscach gdzie może dojść do nieautoryzowanego dostępu ze strony osób trzecich.

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.
Identyfikatory i hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych przechowywane są w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie kierownik Uczelnianego Ośrodka Obliczeniowego oraz Główny Specjalista ds. Informatyki i Aparatury Naukowej. Identyfikatory osób uprawnionych do wykonywania prac administracyjnych oraz hasła są przechowywane w opieczętowanej kopercie. W przypadku konieczności awaryjnego użycia
nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniałą sytuację w „Dzienniku haseł" znajdującym się w szafie wraz z kopertą, w której znajdują się hasła.
Wpis powinien zawierać następujące informacje:
- imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
- imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
- krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać uczelnianego administratora bezpieczeństwa.

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

Przed rozpoczęciem pracy oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia szczególnej uwagi, czy nie wystąpiły przesłanki mogące świadczyć o naruszeniu ochrony danych osobowych.
O naruszeniu ochrony danych osobowych mogą świadczyć następujące przesłanki:
- brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
- brak możliwości zalogowania się do tej aplikacji,
- 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,
- wygląd aplikacji inny niż normalnie,
- inny zakres danych niż normalnie dostępny dla użytkownika
- znaczne spowolnienie działania systemu informatycznego,
- pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,

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

Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
Maksymalna ilość 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. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z lokalnym administratorem bezpieczeństwa informacji.
W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut stacja jest automatycznie blokowana. Odblokowanie stacji jest możliwe przez wprowadzenie hasła.
Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.
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. W pomieszczeniach, w których przetwarzane są dane 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.
Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji i stacji roboczej.

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

Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych

odpowiadają osoby wskazane przez Kierownika Uczelnianego Ośrodka Obliczeniowego.
Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:
Kopie zapasowe wykonywane są codziennie pomiędzy godziną 00:00, a godziną 05:00, na zewnętrzne nośniki danych, inne niż te służące do ich bezpośredniego przetwarzania. Do przechowywania kopii zapasowych służą:
• Serwer KOPIE – na który to serwer dane oraz programy służące ich przetwarzaniu są kopiowane codziennie, i są przechowywane przez okres 60 dni od daty ich wykonania. Kopiowanie danych przebiega z wykorzystaniem sieci teleinformatycznej nie mającej bezpośredniego połączenia z siecią publiczną. Dostęp do serwera chroniony jest poprzez system użytkowników i haseł, oraz poprzez nadawanie tym użytkownikom odpowiednich uprawnień do sporządzania, odczytu oraz odtwarzania kopii zapasowych. Fizyczny dostęp do serwera zabezpieczony jest poprzez umiejscowienie go w pokoju nie posiadającym okien, oraz poprzez system alarmowy. Serwer umieszczony jest w innym budynku niż serwery na których przetwarzane są dane osobowe. Dostęp do pomieszczenia posiadają tylko wybrani administratorzy CI.
• Tandberg SLR – zewnętrzny streamer, posiadający 8 taśm o pojemności 140 GB (z kompresją), na który archiwizowane są dane oraz programy służące ich przetwarzaniu. Archiwizacja przebiega codziennie, dane są kopiowane przy wykorzystaniu programu Veritas Backup Servers, który zainstalowany jest na serwerze KOPIE. Urządzenie zainstalowane jest w tym samym pomieszczeniu co serwer KOPIE. Dostęp fizyczny do urządzenia zabezpieczony jest identycznie jak w przypadku serwera KOPIE,
• Dane z pierwszego dnia roboczego każdego miesiąca, umieszczane są na optycznym nośniku danych DVD.

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 sieci komputerowej.
Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w pkt. 4

Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem.
Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.

Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza teren kampusu uczelnie powinno odbywać się za wiedzą administratora bezpieczeństwa informacji.
W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych.
Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.
W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych
Elektroniczne nośniki danych nie stanowiące trwałego wyposażenia komputerów przechowywane są w zamkniętych szafach i pozostają pod opieką lokalnych administratorów bezpieczeństwa informacji.
Elektroniczne nośniki zawierające kopie zapasowe przechowywane są w ognioodpornym sejfie, do którego dostęp posiadają wyłącznie Kierownik Uczelnianego Ośrodka Obliczeniowego oraz Główny Specjalista ds. Informatyki i Aparatury Naukowej.N ośniki te przechowywane są przez okres minimum 5-ciu lat.

6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III załącznika do rozporządzenia.

W celu przeciwdziałania oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego wprowadzone są następujące zabezpieczenia:
- odseparowanie serwerów bazy danych od sieci zewnętrznej,
- autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
- stosowaniu aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
- stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
- stosowanie odpowiedniej ochrony antywirusowej i ochrony zapór ogniowych na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych,
- stosowanie wyłącznie licencjonowanego oprogramowania

Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

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:
- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony,
- skaner poczty elektronicznej powinien być stale włączony.

Systemy antywirusowe zainstalowane na stacjach roboczych skonfigurowane są w sposób uniemożliwiający ingerencję użytkownika w ustawienia oprogramowania
System zapewnia centralne uaktualnienia wzorców wirusów.
System antywirusowy jest aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.
Użytkownicy systemu informatycznego zobowiązani są do następujących działań:
- skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów
- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
- skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

7. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia:

System informatyczny przetwarzający dane osobowe 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).
System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych:
- data pierwszego wprowadzenia danych osobowych do zbioru
- identyfikator osoby wprowadzającej te dane
- źródło danych (w przypadku pozyskania nie od osoby, której te dane dotyczą)
- informacja o udostępnieniu danych osobowych

- sprzeciw dotyczący przetwarzania danych osobowych
- sporządzania i wydrukowania raportu

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

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.
Prace serwisowe są wykonywane wyłącznie przez pracowników Uczelnianego Ośrodka Obliczeniowego lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie pracowników Uczelnianego Ośrodka Obliczeniowego.
Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej

Wszelkie przeglądy i konserwacje stacji roboczych wykonywane są na bieżąco po wcześniejszym zgłoszeniu upoważnionemu pracownikowi Uczelnianego Ośrodka Obliczeniowego.
Przeglądy i konserwacje serwerów wykonywane są w cyklach tygodniowych.
Monitorowanie stanu pracy serwerów, w tym stanu dysków wykonywane jest ciągle przez administratorów systemów.
W przypadku konieczności wyłączenia pracy serwera na krótki okres czasu, użytkownicy powiadamiani są przez administratorów z minimum 30 minutowym wyprzedzeniem.
W przypadku konieczności wyłączenia serwera na okres dłuższy niż 1 godzina użytkownicy powiadamiani są z dwudniowym wyprzedzeniem.

Załącznik 1 do Instrukcji:

Wzór upoważnienia

UPOWAŻNIENIE

Upoważniam Panią/Pana ....
zatrudnioną/ego na w jednostce organizacyjnej
.....
do przetwarzania danych osobowych
w systemie informatycznym w programie ....., w zakresie wynikającym z zakresu obowiązków służbowych.
Niniejsze upoważnienie jest ważne do dnia ..... .

Jednocześnie uprzejmie informuję, że zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) osoby, które zostały upoważnione do przetwarzania danych są obowiązane zachować w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczenia.

.....
(podpis administratora danych osobowych)

.....
(podpis osoby, której upoważnienie dotyczy)