Załącznik nr 1 do zarządzenia nr 61/2020
Rektora Uniwersytetu Opolskiego z dnia 29 maja 2020 r.

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
W UNIWERSYTECIE OPOLSKIM

SPIS TREŚCI

I. Informacje ogólne

Tworzy się niniejszy dokument o nazwie Instrukcja Zarządzania Systemem Informatycznym (zwany dalej „Instrukcją") w Uniwersytecie Opolskim, której celem jest ustanowienie zasad zarządzania systemem informatycznym, w którym przetwarzane są dane z szczególnym uwzględnieniem danych osobowych, jak również warunków organizacyjnych i technicznych, jakie spełniać powinny, wchodzące w jego skład urządzenia, biorąc pod uwagę skalę zagrożeń i kategorie danych objęte ochroną.

Zgodnie z przepisami rozporządzenia PE 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 oraz uchylenia dyrektywy 95/46/WE Uniwersytet Opolski jest administratorem danych osobowych.

Przestrzeganie zasad instrukcji ma na celu zapewnienie bezpieczeństwa przetwarzanych danych w Uczelni, rozumianego jako zapewnienie: poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.

Procedury określone w niniejszej instrukcji opracowano w odniesieniu do nadrzędnych zasad wynikających z ogólnego rozporządzenia o ochronie danych, w tym w szczególności do zasady rozliczalności, zgodnie, z którą administrator danych ma obowiązek wykazać przestrzeganie zasad ochrony danych osobowych wskazanych w art. 5 ust. 1 ogólnego rozporządzenia o ochronie danych.

Instrukcja przyjęta przez Administratora do stosowania, stanowi obowiązujący wszystkich pracowników i współpracowników dokument.

I.1. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych, przez Administratora Danych – w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
Niniejsza instrukcja określa ogólne zasady zarządzania **każdym systemem informatycznym**, w którym są przetwarzane dane osobowe w Uniwersytecie Opolskim oraz stanowi podstawę do opracowania szczegółowych instrukcji dla każdego z użytkowanych w UO systemów informatycznych służących do przetwarzania danych osobowych.

I.2. Definicje

Ilekroć w instrukcji jest mowa o:

1) **Administrator (AD)** – rozumie się przez to Uniwersytet Opolski decydujący o celach i sposobach przetwarzania danych osobowych,
2) **Lokalny Administrator Danych Osobowych (LADO)** – rozumie się przez to:
   a) Kanclerza Uniwersytetu Opolskiego – w zakresie podległych mu jednostek oraz osób i podmiotów współpracujących,
   b) Kwestora Uniwersytetu Opolskiego – w zakresie podległych mu jednostek oraz osób i podmiotów współpracujących,
   c) Dziekanów / Dyrektorów Instytutów – w zakresie podległych im jednostek oraz osób i podmiotów współpracujących, a także w zakresie doktorantów i studentów wydziałów/instytutów oraz innych osób kształcących się na wydziale / w instytucie,
   d**) Dyrektorów / Kierowników** jednostek ogólnouczelnianych oraz **Kierowników projektów** – w zakresie podległych im pracowników, doktorantów i studentów Uniwersytetu Opolskiego, innych osób kształcących się w Uniwersytecie Opolskim oraz innych osób korzystających z usług świadczonych przez te jednostki,

e) Dyrektora Centrum Informatycznego Uniwersytetu Opolskiego – w zakresie podległych mu osób oraz podmiotów współpracujących;

3) **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora Danych na podstawie art. 37, do wypełnienia zadań, o których mowa w art. 39 RODO,

4) **Administrator Systemów Informatycznych (ASI)** – rozumie się przez to Dyrektora Centrum Informatycznego Uniwersytetu Opolskiego. ASI koordynuje działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w szczególności zawierających programy lub bazy danych zastosowane do przetwarzania danych osobowych. ASI odpowiada za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach wykorzystywanych przez Administratora Danych, również w przypadku dostępu zdalnego i mobilnego do systemu, w szczególności z użyciem sieci Internet lub radiowej sieci bezprzewodowej, w tym z użyciem prywatnych urządzeń użytkowników, w sytuacjach gdy zostało to dozwolone przez AD,

5) **Lokalny Administrator Systemu Informatycznego (LASI)** – rozumie się przez to wyznaczonych przez ASI administratorów systemu informatycznego oraz administratorów systemów informatycznych w jednostkach Uniwersytetu Opolskiego, LASI powoływany jest przez Administratora Systemów Informatycznych, w przypadku gdy dotyczy to systemów informatycznych w jednostkach organizacyjnych – w uzgodnieniu z właściwym Lokalnym Administratorem Danych Osobowych,

6) **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

7) **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

8) **przetwarzanie –** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

9) **obszarze przetwarzania danych osobowych –** rozumie się przez to pomieszczenia, w których przetwarza się dane osobowe w Uniwersytecie Opolskim,

10) **użytkowniku –** rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano w systemie informatycznym identyfikator i przyznano hasło,

11) **odbiorcy** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub obowiązującym w Polsce przepisem prawa nie są jednak uznawane za odbiorców, przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

12) **osobie upoważnionej do przetwarzania danych osobowych –** rozumie się przez to osobę, która została upoważniona do przetwarzania danych osobowych,

13) **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora,

14) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,

15) l**ogin** (**identyfikator**) – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących w konkretnym systemie informatycznym osobę upoważnioną do przetwarzania danych osobowych,

16) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

17) **poufności danych –** rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

18) **dostępności** – należy przez to rozumieć zapewnienie, że dane są możliwe do wykorzystania zawsze, gdy podmiot uprawniony tego potrzebuje,

19) **rozliczalności –** rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

20) **raporcie** – rozumie się przez to przygotowane zestawienia zakresu i treści przetwarzanych danych w systemie informatycznym,

21) **sieci publicznej –** rozumie się przez to sieć publiczną w zakresie ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2019 r. poz. 2460, ze zm..),

22) **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w zakresie ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tj. Dz. U. z 2019 r. poz. 2460, ze zm.),

23) **serwisancie –** rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego i oprogramowania,

24) **teletransmisji –** rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

25) **uwierzytelnianiu –** rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

26) **bezpośrednim dostępie do systemu informatycznego –** rozumie się przez to dostęp bez użycia dodatkowych metod autoryzacji (np. dostęp do plików baz danych),

27) **przetwarzaniu w sposób tradycyjny –** rozumie się przez to przetwarzanie danych przechowywanych poza systemami informatycznymi UO (np. teczki pracownicze, dokumenty gromadzone w segregatorach itp.),

28) **Intranet –** rozumie się przez to wydzieloną wewnątrz UO sieć komputerową, w której umieszczone są serwery i stacje robocze na których przetwarza się dane osobowe w UO.

II. System Informatyczny

SYSTEM INFORMATYCZNY – jest to część systemu przetwarzania danych w Uczelni, który zawiera się w systemie informacyjnym.

System informatyczny realizowany jest dzięki technologii komputerowej, stanowi zbiór powiązanych ze sobą elementów, takich jak zespoły współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych, jak również przepływu tych danych.

Na systemy informatyczne składają się takie elementy jak:

1) sprzęt – w Uczelni głównie **komputery**, oraz:
    a) urządzenia służące do przechowywania danych,
    b) urządzenia służące do zbierania danych – kamery, sensory,
    c) urządzenia służące do komunikacji między sprzętowymi elementami systemu,
    d) urządzenia służące do komunikacji między ludźmi a komputerami,
    e) urządzenia służące do odbierania danych ze świata zewnętrznego – *nie od ludzi* (na przykład czujniki elektroniczne, kamery, skanery),
    f) urządzenia służące do wywierania wpływu przez systemy informatyczne na świat zewnętrzny – elementy wykonawcze
    g) urządzenia służące do przetwarzania danych nie będące komputerami,
2) Oprogramowane,
3) zasoby osobowe – pracownicy, współpracownicy uczelni, studenci (administratorzy i użytkownicy systemu) ludzie oddziaływujący na system.,
4) elementy organizacyjne – czyli procedury korzystania z systemu informatycznego, instrukcje robocze itp.,
5) elementy informacyjne; bazy wiedzy – ontologie dziedziny/dziedzin, w których używany jest system informatyczny – na przykład podręcznik księgowania w wypadku systemu finansowo-księgowego.

Systemy informatyczne użytkowane w Uczelni mogą być bardzo proste – np.: pojedynczy system komputerowy działający autonomicznie, jak i złożone – na przykład system obsługi studiów (USOS) czy system finansowo-księgowy.
Miarą złożoności systemu może być na przykład ilość elementów systemu połączona ze złożonością stosowanego oprogramowania mierzoną w ilości punktów funkcyjnych.

Każdy system informatyczny w Uczelni administrowany jest przez LASI, w przypadku gdy jest to pojedynczy komputer AD/LADO może powierzyć obowiązki LASI – użytkownikowi komputera (w przypadku gdy jest on współużytkowany – głównemu użytkownikowi).

III. Poziom bezpieczeństwa

Miarą bezpieczeństwa jest **wielkość ryzyka** związanego z ochroną danych osobowych.

LASI (w współdziałaniu z ASI -w przypadku systemów ogólnouczelnianych, LADO – w przypadku systemów lokalnych – użytkowanych w jednostce organizacyjnej) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych, których dane osobowe są przetwarzane w administrowanym systemie informatycznym, zgodnie z obowiązującą Polityką Zarządzania Ryzykiem w Uniwersytecie Opolskim z uwzględnieniem zasad opisanych w załączniku nr 16 do Polityki Bezpieczeństwa Danych Osobowych w Uniwersytecie Opolskim.

Przyjmuje się, iż akceptowalnym poziom ryzyka jest to poziom niski

W przypadku gdy określono **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych w ogólnouczelnianym systemie informatycznym, lub **ze względu na rodzaj przetwarzania jest ona obligatoryjna,** ASI w współdziałaniu z IOD przeprowadza „ Ocenę skutków dla ochrony danych" zgodnie z załącznikiem nr 17 do Polityki Bezpieczeństwa Danych Osobowych w Uniwersytecie Opolskim.

W przypadku gdy określono **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych lub **ze względu na rodzaj przetwarzania jest ona obligatoryjna**, w systemach użytkowanych w jednostkach organizacyjnych „Ocenę skutków dla ochrony danych" prowadzi **LADO** w współdziałaniu z IOD z uczestnictwem LASI.

W przypadku gdy określone ryzyko jest średnie lub poważne ww. osoby funkcyjne poprzez zarządzanie ryzykiem **zobowiązane są do uzyskania poziomu akceptowalnego.**

IV. Wymagania Bezpieczeństwa

1. Bezpieczeństwo powinno być integralną częścią systemów informatycznych służących do przetwarzania danych osobowych.
2. Aplikacje oraz usługi, które nie są wykorzystywane powinny być wyłączone.
3. Krytyczne poprawki bezpieczeństwa powinny być przetestowane i zainstalowane.
4. Dostęp do poszczególnych usług systemów informatycznych powinien być zabezpieczony za pomocą kontroli dostępu.
5. Wymagania bezpieczeństwa, na które mogą się również składać wymagania prawne związane z ochroną danych osobowych, należy identyfikować i uzgodnić przed opracowaniem i/lub ich wdrożeniem. W szczególności wymagania muszą być zidentyfikowane dla:
   a) systemów operacyjnych;
   b) aplikacji;
   c) poszczególnych usług.
   d) narzędzi programowych;
   e) baz danych;
   f) infrastruktury teleinformatycznej;

6. Aplikacje przeglądarkowe przed wdrożeniem powinny zostać poddane przeglądowi bezpieczeństwa mającemu na celu zidentyfikowanie podatności na zagrożenia pochodzące z sieci Internet.

V. Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

Szczegółową procedurę postępowania nadawania i wyrejestrowania uprawnień zawiera załącznik nr 4 do Polityki Bezpieczeństwa Danych Osobowych w Uniwersytecie Opolskim.
Procedurę stosuje się również w przypadku gdy użytkownik systemu nie będzie przetwarzał danych osobowych w systemie.

1. Uprawnienia do systemu informatycznego nadawane są z zachowaniem następujących zasad:

a) Minimalnych przywilejów każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków,

b) Wiedzy koniecznej pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań,

c) Domniemanej odmowy wszystkie działania, które nie są jawnie dozwolone są zabronione.

2. Każdy zarejestrowany użytkownik korzysta z przydzielonego mu konta użytkownika, opatrzonego identyfikatorem (login) i hasłem dostępu.
3. Aby zapewnić zasadę rozliczalności wynikającą z rozporządzenia ogólnego każdy użytkownik systemu informatycznego jest jednoznacznie identyfikowany poprzez nadany mu indywidualny identyfikator (login) użytkownika.
4. Zabronione jest korzystanie z tego samego identyfikatora (loginu) przez więcej niż jednego użytkownika.
5. LASI lub osoba upoważniona przez LADO ma obowiązek prowadzenia rejestru osób upoważnionych do korzystania z systemów informatycznych
6. Rejestr, o którym mowa powyżej prowadzony jest w postaci elektronicznej lub papierowej.
7. Przykładowy rejestr umieszczono w załączniku nr 1 do Instrukcji Zarządzania Systemem informatycznym (jest on obowiązujący w przypadku prowadzenia rejestru w wersji papierowej).
8. LASI lub osoba upoważniona przez LADO raz na 30 dni dokonuje przeglądu stanu aktywności kont użytkowników.
9. Na potrzeby „awaryjnego" administrowania systemem tworzone są uniwersalne konta administracyjne typu „admin".
10. Identyfikatory i hasła kont administracyjnych tworzonych w trybie pkt 9 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, w jednostkach organizacyjnych – LADO i jego zastępcy. Identyfikatory oraz hasła uprawniające do wykonywania prac administracyjnych są przechowywane w oznakowanej i podpisanej kopercie.
11. W przypadku konieczności awaryjnego użycia nazw i haseł konta typu „admin" 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, w jednostkach organizacyjnych odpowiednio LADO lub jego zastępcy.
12. Po ustaniu konieczności awaryjnego użycia konta typy „admin", ASI/LASI dokonują zmiany hasła do konta awaryjnego.
13. Wpis, o którym mowa w pkt.11, powinien zawierać następujące informacje:
    - imię i nazwisko oraz stanowisko osoby upoważnionej umożliwiającej 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.

V.1. Sposób nadawania i rejestrowania uprawnień.

1) Dostęp do systemu informatycznego w którym przetwarzane są dane osobowe może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana, jako użytkownik w tym systemie przez LASI na wniosek Kierownika właściwej jednostki organizacyjnej, w której przetwarzane są dane.
2) Wzór wniosku stanowi załącznik nr 5 do Polityki Bezpieczeństwa Danych Osobowych w Uniwersytecie Opolskim.
3) Administrator Systemu Informatycznego/Lokalny Administrator Systemu Informatycznego jest zobowiązany upoważnić co najmniej jednego pracownika Centrum

Informatycznego lub inną osobę wskazana przez ASI/LADO do rejestracji uprawnień w systemie informatycznym w czasie swojej nieobecności dłuższej niż 14 dni.

4) Rejestracja użytkownika, o której mowa w ust. 1), polega na nadaniu unikalnego w ramach systemu identyfikatora, przydzieleniu hasła oraz nadaniu uprawnień wynikających z zakresu obowiązków danej osoby i musi być z godna z zakresem obowiązków opisanym we wniosku o nadanie uprawnień.
5) ASI/ASI lub upoważniony pracownik, o którym mowa w ust. 3), przekazuje do LADO (IOD) identyfikator nadany użytkownikowi.

V.2. Sposób wyrejestrowywania uprawnień.

1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego/Lokalny Administrator Systemu Informatycznego lub wyznaczony przez ASI pracownik, na wniosek Kierownika jednostki organizacyjnej, który wnioskował o rejestrację użytkownika w systemie, lub na wniosek jego przełożonego.
2) Wzór wniosku stanowi załącznik nr 5 do Polityki Bezpieczeństwa Danych Osobowych w Uniwersytecie Opolskim.
3) Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
4) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie uprawnień, zmiana hasła i zablokowanie konta w systemie informatycznym (wyrejestrowanie trwałe).
5) Czasowe wyrejestrowanie użytkownika z systemu informatycznego może nastąpić w razie:
   a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych,
6) Przyczynami czasowego wyrejestrowanie użytkownika z systemu informatycznego mogą być:
   a) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych,
   b) zmiana zakresu obowiązków,
   c) przeniesienie na inne stanowisko pracy
7) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik lub zmiana zakresu obowiązków pracowniczych.
8) Kierownicy jednostek organizacyjnych, na wniosek których udzielono upoważnienia zobowiązani są, w przypadku pojawienia się jakiejkolwiek z przyczyn ograniczenia uprawnień pracownika, do zgłoszenia tego faktu Administratorowi Systemu Informatycznego/Lokalnemu Administratorowi Systemu Informatycznego.

V.3. Konto uprzywilejowane.

1) Nadawane przywileje, czyli większe uprawnienia niż wynika to z realizowanych zadań użytkownika podlegają ścisłej ewidencji prowadzonej przez LASI lub osobę upoważnioną przez LADO.
2) Konta użytkownika uprzywilejowanego należy oznaczyć, zapewnić ich łatwą identyfikację oraz zapewnić, że odwołują się do jednego użytkowania.

3) Konto uprzywilejowane nie może służyć do realizacji przez użytkownika standardowych zadań.
4) Czynności wykonywane za pomocą kont uprzywilejowanych należy rejestrować oraz zapewnić możliwości ich identyfikacji i rozliczalności.
5) Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.
6) Konta uprzywilejowane podlegają regularnym przeglądom i kontroli prowadzonym przez LASI/LADO.

VI. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

VI.1. Login – Identyfikator

1) Identyfikator składa się z liter, z których pierwsza część odpowiada stanowi imię użytkownika, a kolejne są jego nazwiskiem i informacją o nazwie domenowej (@uni.opole.pl). W identyfikatorze pomija się polskie znaki diakrytyczne, które są zastępowane łacińskimi literami.
2) W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, LASI, nadaje inny identyfikator, odstępując od zasady określonej w ust. 1).
3) Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi systemu.
4) Ze względu na wymogi systemu dotyczące formy loginu, LASI w instrukcji systemu może określić inne zasady tworzenia identyfikatora niż to ujęto w pkt 1.

VI.2. Hasło użytkownika

Hasło użytkownika powinno składać się z unikalnego zestawu **co najmniej ośmiu** znaków, zawierać małe i wielkie litery oraz przynajmniej jedną cyfrę i znak specjalny. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

1) Pierwsze hasło użytkownika określa LASI, przekazuje je użytkownikowi wraz z informacją dotyczącą loginu i sposobu logowania się do systemu.
2) Należy stosować bezpieczną procedurę przekazywania haseł użytkownikom np. nieprzesyłanie haseł przez sieć (np. w niechronionych wiadomościach poczty elektronicznej).
3) Hasło, o którym mowa w pkt 1 musi być zmienione przez użytkownika, po pierwszym udanym zalogowaniu się do systemu informatycznego,
4) Kolejne hasła są zmieniane przez użytkownika, hasła dostępu do systemu tworzone przez użytkownika, stanowią tajemnicę znaną wyłącznie temu użytkownikowi, i nie powinno powtarzać się częściej niż co 12 miesięcy,
5) Haseł nie powinno się przechowywać w systemach, aplikacjach, bazach danych, skryptach i plikach konfiguracyjnych w postaci jawnej, nie zapewniającej im poufności.
6) Haseł nie powinno się przesyłać za pomocną narzędzi i usług teleinformatycznych w postaci jawnej, nie zapewniającej im poufności.
7) System informatyczny powinien być wyposażony jest w mechanizmy wymuszające zmianę hasła w ustalonych odstępach czasu, nie dłuższych niż 30 dni od dnia ostatniej zmiany hasła,
8) System informatyczny powinien być wyposażony w mechanizmy pozwalające na wymuszenie jakości hasła i zasad powtarzalności,
9) W przypadku gdy system nie posiada mechanizmów wymuszających zmianę hasła w ustalonych odstępach czasu, obowiązek zmiany na zasadach ujętych w punkcie 3 leży po stronie użytkownika. LASI ma obowiązek monitowania twórców systemu o konieczności wprowadzenia ww. mechanizmu i jego aktywacji natychmiast po uzyskaniu takiej możliwości.

10) Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej.
11) Hasła dostępu do aplikacji, przy każdym logowaniu, powinny być wpisywane z klawiatury.
12) Hasło nie powinno zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.
13) Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
14) Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym, zabrania się użytkownikom systemu oraz osobom upoważnionym do przetwarzania danych osobowych korzystania z identyfikatora lub hasła innego użytkownika.
15) Hasło użytkownika należy utrzymywać w tajemnicy, również po upływie jego ważności.
16) W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów do powiadomienia o tym fakcie AD/LADO i IOD.
17) Zabronione jest przechwytywanie lub odgadywaniem haseł innych użytkowników.

Użytkownik będący jednocześnie LASI powinien posiadać dodatkowo konto służące tylko i wyłącznie do administracji danym systemem informatycznym zwane kontem administracyjnym, hasło do tego konta musi spełniać wymogi hasła administratora.

VI.3. Hasło administratora

Hasło Administratora systemu informatycznego oraz użytkownika uprzywilejowanego powinno składać się z unikalnego zestawu co najmniej dwunastu znaków, zawierać małe i wielkie litery oraz przynajmniej jedną cyfrę i znak specjalny.
Zasady zarządzania hasłami i ochrony są analogiczne, jak w przypadku haseł użytkowników

VII. 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. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy przystąpić do realizacji czynności zgodnie z Procedurą postępowania w przypadku naruszenia ochrony danych osobowych – załącznik nr 18 do Polityki Bezpieczeństwa Danych Osobowych Uniwersytetu Opolskiego.

VII.1. Tryb pracy na stacjach roboczych.

1) Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia jeśli występują kolejno w listwie podtrzymującej napięcie lub zasilacza awaryjnego (UPS) i stacji roboczej, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora.
2) W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika upoważnionego do przetwarzania danych osobowych albo LADO/IOD.
3) Przed osobami postronnymi należy chronić ekrany stacji roboczych (ustawienie monitora powinno uniemożliwiać pogląd ekranu), wydruki leżące na biurkach oraz w otwartych szafach.
4) Monitory stacji roboczych wyposażone muszą być we włączające się po maksimum 5 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
5) W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywować wygaszacz ekranu lub w inny sposób zablokować stację roboczą (sekwencja klawiszy Win+L lub CTR+ALT+DEL).
6) Obowiązuje zakaz robienia kopii całych zbiorów danych; całe zbiory danych mogą być kopiowane tylko przez ASI/LASI lub automatycznie przez oprogramowanie do wykonywania kopii zapasowych, z zachowaniem procedur ochrony danych osobowych.
7) Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach.
   Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
8) Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami administratora danych a komputerami przenośnymi użytkowników tylko po ich zaszyfrowaniu.
9) Przesyłanie danych osobowych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.
10) Obowiązuje zakaz wynoszenia poza teren UO na jakichkolwiek nośnikach całych zbiorów danych osobowych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
11) W przypadku braku centralnej archiwizacji zbiorów danych osobowych przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak by zapobiec ich utracie.

12) Zakończenie pracy na stacji roboczej następuje po zatwierdzeniu wprowadzonych tego dnia danych, a następnie prawidłowym wylogowaniu się użytkownika z aplikacji oraz wyłączeniu komputera oraz odcięciu napięcia w listwie zasilającej lub zasilaczu awaryjnym (UPS).
13) Przed opuszczeniem pokoju należy:
    a) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
    b) schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,
    c) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
    d) zamknąć okna i jeśli są wyposażone w kraty, żaluzje antywłamaniowe należy ich użyć,
14) Opuszczając pokój, należy zamknąć za sobą drzwi na klucz. Klucz od pokoju przechowywany jest na portierni.

VII.2. Tryb pracy na komputerach/urządzeniach przenośnych.

1) Przy przetwarzaniu danych osobowych na komputerach* przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na stacjach roboczych.
2) Użytkownicy, którym zostały powierzone komputerach/urządzeniach przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.
3) Obowiązuje zakaz używania komputerów przenośnych przez osoby inne, niż użytkownicy, którym zostały one powierzone.
4) Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.
5) Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni.
6) Pliki zawierające dane osobowe przechowywane na komputerach przenośnych muszą być zaszyfrowane i opatrzone hasłem dostępu.
7) Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
8) Użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na serwerze AD, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.
9) Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem ASI/LASI, stosownie do wymagań niniejszej instrukcji.
10) Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.
11) Użytkownik urządzenia przenośnego odpowiada za bieżącą aktualizacje oprogramowania systemu operacyjnego oraz zainstalowanych aplikacji użytkowych.
12) Dodatkowe obostrzenia mogą być nałożone na użytkownika komputera przenośnego w ramach istniejących na UO instrukcji.

**-Słowo komputer w powyższych punktach oznacza również inne urządzenia przenośne takie jak: tablety, smartfony itp.*

Podczas użytkowania komputera przenośnego (Laptopa), poza obszarem UO, zalecane się stosowanie nakładki prywatyzujące na ekran minimalizujące ryzyko wglądu w ekran osobom postronnym.

VII.3. Procedura zdalnego dostępu do systemów informatycznych

Procedura opisuje możliwości zdalnego dostępu do systemów informatycznych AD, którego celem może być świadczenie usługi wsparcia technicznego lub utrzymania systemu informatycznego.

1. Do nawiązywania zdalnych połączeń administracyjnych muszą być stosowane:
   a) rozwiązania komunikacyjne bazujące na bezpiecznych standardach komunikacji zapewniające szyfrowanie transmisji;
   b) użytkownik systemu musi zezwolić na autoryzacje zdalnego połączenia poprzez podanie id sesji oraz hasła dostępowego;
   c) użytkownik inicjujący zdalne połączenie zobowiązany jest nadzorować proces zdalnego połączenia;
   d) po zakończeniu pracy zdalnej sesja musi zostać zamknięta.
2. W przypadku możliwości technicznych Administratora akceptuje się możliwość wykorzystania protokołu VPN umożliwiającego podłączenie do sieci Administratora bez każdorazowej autoryzacji użytkownika.
3. Utworzenie konta VPN możliwe jest tylko i wyłącznie za zgodą ASI.
4. Rozwiązanie służące do komunikacji VPN musi mieć możliwość logowania sesji zdalnych użytkowników.

Zdalny dostęp do systemów informatycznych w innych celach niż wskazane powyżej (np. zdalna praca) wymaga pisemnej zgody Rektora lub Kanclerza Uniwersytetu Opolskiego.

AD (LADO) organizując pracę zdalną może określić dodatkowe zasady dotyczące trybu pracy i wykorzystania sprzętu komputerowego.

VII.4. Zasady korzystania ze służbowej poczty elektronicznej

1. Każdy pracownik Uniwersytetu Opolskiego przy prowadzeniu korespondencji służbowej oraz korzystania z systemów informatycznych wykorzystywanych na UO zobowiązany jest do posługiwania się służbowym adresem e-mail w domenie uni.opole.pl.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora Danych.
3. Konto e mail służy wyłącznie do realizacji celów służbowych lub umownych.
4. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora Danych może podlegać rejestrowaniu i monitorowaniu.
5. Informacje przesyłane za pośrednictwem sieci (w tym do i z Internetu) z wykorzystaniem służbowej poczty elektronicznej, nie stanowią własności prywatnej użytkownika.
6. Użytkownicy dokonujący wysyłki korespondencji masowej, obowiązani są do ukrywania adresatów wiadomości w polu UDW.
7. Zabronione jest:
   a) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
   b) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Uczelni;
   c) odbieranie przesyłek z nieznanych źródeł;
   d) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   e) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików

multimedialnych

f) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika*;
g) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją ASI;
h) posługiwanie się adresem służbowym e mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
i) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo usługowej innej niż wynikającej z potrzeb AD lub do poszukiwania dodatkowego zatrudnienia.

**Nie dotyczy pracowników CI – administratorów Uczelnianego systemu pocztowego.*

Tworzenie kont i ogólne zasady korzystania z służbowej poczty elektronicznej zawarte zostały w § 4 Regulaminu korzystania z Sieci Komputerowej Uniwersytetu Opolskiego (Regulamin SKUO)

VII.5. Korzystanie z sieci Internet

1. Urządzenia komputerowe oraz działają systemy informatyczne Administratora musi być odseparowana od sieci publicznej zaporą ogniową (firewall) lub (i) urządzeniem typu UTM.
2. Systemy informatyczne w których przetwarzane są dane osobowe powinny korzystać z szyfrowanych protokołów wymiany danych np. https.
3. Dostęp użytkowników do sieci publicznej powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Dostęp do protokołu wymiany plików np. ftp możliwy jest w uzasadnionych przypadkach, po nadaniu odpowiednich uprawnień.

Dalsze ograniczenia dostępu do sieci Internet zawarte zostały w Regulaminie korzystania z Sieci Komputerowej Uniwersytetu Opolskiego, mogą być również rekomendowane przez IOD.

VIII. Tworzenia kopii zapasowych

Kopie zapasowe tworzone są zgodnie z Polityką Tworzenia Kopii Zapasowych Uniwersytetu Opolskiego.

Kopia zapasowa nie stanowi kopii archiwalnej danych z systemu

I. W systemach informatycznych wykorzystujących technologię klient-serwer kopie zapasowe wykonuje się po stronie serwera. Dostęp do kopii bezpieczeństwa mają tylko ASI/LASI oraz upoważnieni pracownicy Centrum Informatycznego.
II. Kopie zapasowe systemów klienckich (na stacjach roboczych za wyjątkiem terminali) wykonują osoby korzystające z tych systemów.

1. Kopie zapasowe tworzy się na oddzielnych nośnikach informatycznych.
2. Nośniki zawierające kopie zapasowe należy oznaczać jako „Kopia zapasowa dzienna/tygodniowa/miesięczna" wraz z podaniem daty sporządzenia i nazwy systemu.
3. Częstotliwość wykonywania kopii – realizowana zgodnie z Polityką Tworzenia Kopii Zapasowych Uniwersytetu Opolskiego.

VIII.1. Testowanie kopii

W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy, co najmniej raz na sześć miesięcy poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.

VIII.2. Przechowywanie kopii

1) Kopie zapasowe z pkt I przechowuje się w wydzielonych pomieszczeniach CI z zainstalowanym system wykrywania pożaru i rejestratorem dostępu.. Dostęp do tych kopii posiada wyłącznie ASI/LASI, upoważnieni pracownicy CI oraz IOD. Każde wydanie i przyjęcie kopii jest odnotowywane w dokumentacji. W przypadku systemów informatycznych tego typu użytkowanych w jednostce organizacyjnej za określenie zasad przechowywania kopii zapasowej odpowiada LADO, dostęp do kopii posiada LASI, pracownicy jednostki upoważnieni przez LADO i IOD.
2) Za przechowywanie kopii zapasowych z pkt II odpowiadają właściciele tych systemów, zaleca się nieprzechowywanie kopii w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Jednocześnie kopie zapasowe muszą być odpowiednio zabezpieczone fizycznie (sejf, zamykane szafy w ognioodporny w zabezpieczonym pomieszczeniu).

VIII.3. Likwidacja nośników zawierających kopie

3) Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.
4) Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.
5) Niszczenie nośników danych powinno się odbywać komisyjnie i być potwierdzone stosownym protokołem.

IX. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1) Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2) Zabrania się wynoszenia poza obszar organizacji wymiennych nośników informacji, a w szczególności dysków twardych i przenośnych pamięci masowych z zapisanymi danymi osobowymi bez pisemnej zgody AD/LADO.
3) Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.
4) Na nośnikach, o których mowa w ust. 2), dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
5) W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.

6) Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej instrukcji.
7) Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.
8) Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny.
9) Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.
10) W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:
    a) adresat powinien zostać powiadomiony o przesyłce
    b) nadawca powinien sporządzić kopię przesyłanych danych
    c) dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą
    d) stosować bezpieczne koperty depozytowe
    e) przesyłkę należy przesyłać przez kuriera lub doręczyć osobiście
    f) adresat powinien powiadomić nadawcę o otrzymaniu przesyłki
11) Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).
12) Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar organizacji (np. serwis, sprzedaż lub darowizna komputerów stacjonarnych / laptopów).

X. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1) W celu przeciwdziałania programom, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego wprowadzone są następujące zabezpieczenia:
    a) odseparowanie serwerów bazy danych od sieci zewnętrznej,
    b) autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
    c) stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
    d) stosowanie aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
    e) stosowanie szyfrowanej transmisji danych,
    f) stosowanie odpowiedniej ochrony antywirusowej i ochrony zapór ogniowych na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych,
    g) stosowanie wyłącznie licencjonowanego oprogramowania.
2) Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
    a) załączniki do poczty elektronicznej,
    b) przeglądane strony internetowe,

c) pliki i aplikacje pochodzące z nieautoryzowanych źródeł, niezabezpieczonych nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.

3) W celu zapewnienia ochrony antywirusowej wyznaczony przez ASI pracownika CI lub LASI. jest odpowiedzialny za zainstalowanie oraz zarządzanie systemem/oprogramowaniem antywirusowym wykrywającym i usuwającym wirusy
4) Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez wyznaczonego przez ASI pracownika CI lub LASI.
5) System antywirusowy powinien być skonfigurowany w następujący sposób:
   a) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej),
   b) antywirusowy skaner ruchu internetowego,
   c) monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office,
   d) skaner poczty elektronicznej,
6) Oprogramowanie, o którym mowa w pkt. 3), sprawuje ciągły nadzór (ciągła praca w tle, elementy systemu wymienione w pkt. 5 powinny być stale włączone) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
7) Systemy antywirusowe zainstalowane na stacjach roboczych skonfigurowane są w sposób uniemożliwiający ingerencję użytkownika w ustawienia oprogramowania. System zapewnia centralne uaktualnienia wzorców wirusów, jest aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.
8) Niezależnie od ciągłego nadzoru, o którym mowa w pkt. 6), administrator systemu nie rzadziej niż raz na miesiąc przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
9) Do obowiązków LASI oraz użytkownika systemu informatycznego należy nadzór nad działaniem i aktualizacją oprogramowania antywirusowego.
10) Użytkownicy systemu informatycznego zobowiązani są do następujących działań:
    a) Zgłaszanie do ASI konieczności instalacja, oprogramowania antywirusowego na przypisanych do niego komputerach stacjonarnych i przenośnych,
    b) skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – na bieżąco,
    c) skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
    d) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.
11) Użytkownik jest obowiązany zawiadomić Administratora Systemu Informatycznego/Lokalnego Administratora Systemu Informatycznego o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
12) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy LASI lub inny wyznaczony pracownik CI, podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
    a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
    b) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
13) Użytkownicy Intranetu mogą korzystać z zewnętrznych nośników danych tylko na stanowisku wydzielonym z sieci komputerowej Administratora Danych po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

14) Dostęp do Internetu w sieci Intranet możliwy jest na stacjach roboczych, specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem Firewall i translacją adresów NAT.

XI. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

System informatyczny Administratora Danych Osobowych powinien umożliwić automatycznie:

1) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
2) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (dotyczy to także komputerów przenośnych),
3) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego:
   a) datę pierwszego wprowadzenia danych do systemu Administratora Danych,
   b) identyfikator użytkownika wprowadzającego te dane,
   c) źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą,
   d) sprzeciwu, o którym mowa w art. 21 RODO.
4) Odnotowanie informacji, o których mowa w ust. 3), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
5) Dla każdej osoby, której dane osobowe przetwarzane są w systemie informatycznym, system ten powinien zapewnić odnotowanie informacji o udostępnieniach danych odbiorcom, w rozumieniu art. 4 pkt 9 RODO, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.
6) Osoba, której dane dotyczą, ma prawo otrzymać (z zastrzeżeniami art. 20 RODO) w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:
   a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO;
   oraz
   b) przetwarzanie odbywa się w sposób zautomatyzowany.

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

1) Przeglądu i konserwacji systemu dokonuje LASI doraźnie, oraz ASI/LADO w ramach prowadzonej działalności kontrolnej.
2) Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) LASI dokonuje nie rzadziej niż raz na tydzień.
3) Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale LASI nie rzadziej niż raz na miesiąc.
4) Zapisy logów systemowych powinny być przeglądane przez LASI codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
5) Kontrole i testy przeprowadzane przez IOD, powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

XIII. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1) Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych przeprowadzane są – o ile to możliwe – przez pracowników Centrum Informatycznego pod nadzorem ASI/LASI.
2) Naprawy i zmiany w systemie informatycznym Administratora Danych w których przetwarzane są dane osobowe, przeprowadzane są przez zewnętrznych serwisantów wyłącznie po wcześniejszym zawarciu umowy powierzenia danych (wzór umowy – załącznik nr 10 Polityki Bezpieczeństwa Danych Osobowych) i upoważnieniu przez procesora serwisantów do przetwarzania danych osobowych). Naprawy i zmiany w systemie informatycznym prowadzone są pod nadzorem ASI.LASI w siedzibie Administratora Danych (jeśli to możliwe) lub poza siedzibą Administratora Danych. Nie jest wymagane zawieraniu umów powierzenia przetwarzania danych osobowych naprawa poza siedzibą AD wyłącznie w przypadku gdy sprzęt zostanie pozbawiony nośników zawierających zapisane dane osobowe, lub dane osobowe na nośnikach zostaną nieodwracalnie usunięte.
3) Jeśli nośnik danych (dysk, pendrive, karta pamięci, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w sposób uniemożliwiający odzyskanie danych**.**

XIV. 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) W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
3) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest przed dopuszczeniem do przetwarzania danych oraz złożyć stosowne oświadczenie, potwierdzające znajomość treści niniejszej instrukcji (załączniki nr 6 lub 7 do Polityki Bezpieczeństwa Przetwarzania danych osobowych w Uniwersytecie Opolskim.
4) 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.
5) 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.
6) 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.
7) Instrukcja podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
8) Przeglądu Instrukcji dokonuje ASI – Dyrektor Centrum Informatycznego w współpracy z wyznaczonym pracownikiem z Zespołu Nadzoru Prawnego i IOD.
9) Przegląd powinien obejmować, w szczególności ocenę adekwatności Instrukcji do:
   - procesów funkcjonujących w strukturach Administratora Danych,
   - obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator.

10) W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Instrukcji obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych, jej przegląd wykonywany jest niezwłocznie.
11) Jeżeli w wyniku przeglądu Instrukcji stwierdzona zostanie konieczność aktualizacji jej zapisów, ASI dokonuje jej aktualizacji.
12) Informacje o wprowadzonych zmianach umieszczane są na stronie internetowej CI.

ZAŁĄCZNIK do Instrukcji Zarządzania Systemem Informatycznym

REJESTR UPRAWNIEŃ DO SYSTEMÓW

Lp.	**Imię i nazwisko osoby uprawnionej**	**Data nadania uprawnienia**	**Data ustania uprawnienia**	**Nazwa systemu/usługi/udziału**	**Identyfikator /login**	**Osoba odpowie-dzialna /LASI/**	**Uwagi**
1	2	3	4	6	6	7	8