M O N I T O R
UNIWERSYTETU WARSZAWSKIEGO

Warszawa, 21 listopada 2007 r. **Nr 9E**

Poz. 372

ZARZĄDZENIE NR 39
REKTORA UNIWERSYTETU WARSZAWSKIEGO

z dnia 15 listopada 2007 r.

w sprawie ochrony danych osobowych
na Uniwersytecie Warszawskim

Na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U z 2002 r. Nr 101, poz. 926 z późn. zm.) zwanej dalej ustawą i § 3 ust. 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwanego dalej „Rozporządzeniem", oraz § 35 Statutu Uniwersytetu Warszawskiego (Monitor UW z 2006 r. Nr 7A) zarządza się, co następuje:

§ 1

1. Rektor Uniwersytetu Warszawskiego powierza pełnienie funkcji Administratora Danych Osobowych, zwanego dalej „ADO", oraz Administratora Bezpieczeństwa Informacji − zastępcy kanclerza
ds. informatycznych, zwanego dalej „ABI".

2. ABI powołuje w jednostkach Lokalnych Administratorów Bezpieczeństwa Informacji, zwanego dalej „LABI" na wniosek:
1) Dziekana, Dyrektora albo Kierownika,
2) Kanclerza w odniesieniu do jednostek administracji centralnej,
3) Dyrektora BUW.

3. ABI nadzoruje przestrzeganie zasad ochrony opisanych w art. 36 ust. 1 ustawy, nadzoruje sposób prowadzenia dokumentacji określonej w § 3 ust.1 rozporządzenia na którą składają się: polityka bezpieczeństwa informacji, zwana dalej „Polityką", stanowiąca Załącznik nr 1 zarządzenia oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", stanowiąca Załącznik nr 2 zarządzenia.

4. LABI odpowiedzialny jest za realizację zadań administratora bezpieczeństwa danych osobowych określonych w ustawie, w odniesieniu do zbiorów danych istniejących w danej jednostce organizacyjnej Uniwersytetu.

§ 2

LABI podejmuje niezbędne działania służące realizacji zabezpieczenia danych osobowych przetwarzanych w poszczególnych zbiorach w jednostce, a w szczególności jest zobowiązany do:
1) działania zgodnie z polityką bezpieczeństwa informacji oraz instrukcją zapewnienia stosowania środków technicznych i organizacyjnych, o których mowa w art. 36 ust. 1 ustawy, zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
2) opracowania szczegółowej instrukcji dla każdego systemu informatycznego administrowanego w jednostce na podstawie Instrukcji.

3) przestrzegania procedur szczegółowych instrukcji zarządzania systemem informatycznym administrowanym w jednostce,
4) zapewnienia stosowania środków bezpieczeństwa, o których mowa w § 6 ust. 5 rozporządzenia,
5) prowadzenia wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych osobowych wg formularza nr 1, stanowiącego integralną część Polityki,
6) prowadzenia opisu struktury zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych,
7) prowadzenia wykazu budynków, pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe wg formularza nr 2, stanowiącego integralną część Polityki
8) prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych wg formularza nr 3, stanowiącego integralną część Polityki**,**
9) wydawania upoważnień do przetwarzania danych osobowych wg formularza nr 5 na podstawie wystawionych wniosków wg formularza nr 4, stanowiących integralną część Polityki.

§ 3

LABI zobowiązany jest do działania zgodnie z Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych w Uniwersytecie Warszawskim, stanowiącą Załącznik nr 3 zarządzenia oraz opracowania szczegółowych instrukcji w tym przedmiocie w odniesieniu do zbiorów danych istniejących w danej jednostce organizacyjnej Uniwersytetu.

§ 4

LABI zobowiązany jest do przestrzegania zaleceń podanych w Załączniku nr 4 zarządzenia, odnoszącym się do bezpieczeństwa sieci LAN/WLAN.

§ 5

Tracą moc:
1) Zarządzenie nr 9 Rektora Uniwersytetu Warszawskiego z dnia 1 września 2004 r. w sprawie ochrony danych osobowych w Uniwersytecie Warszawskim (Monitor UW z 2004 r. Nr 6, poz. 97);
2) Zarządzenie nr 3 Rektora Uniwersytetu Warszawskiego z dnia 13 stycznia 2006 r. o zmianie Zarządzenia nr 9 Rektora UW z dnia 1 września 2004 r. w sprawie ochrony danych osobowych w Uniwersytecie Warszawskim (Monitor UW z 2006 r. Nr 1, poz. 11).

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor UW: *K. Chałasińska-Macukow*

Załącznik nr 1
do zarządzenia nr 39 Rektora UW z dnia 15 listopada 2007 r.
w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim

POLITYKA BEZPIECZEŃSTWA UNIWERSYTETU WARSZAWSKIEGO

1. Podstawa prawna.

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, wraz z dokumentami udostępnionymi przez Generalnego Inspektora Danych Osobowych,
2) 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,
3) Polskie normy w zakresie:
   a) Systemów ochrony informacji: PN-I-07799-2:2005
   b) Systemów zarządzania bezpieczeństwem informacji – część 2: Specyfikacja i wytyczne do stosowania
   c) PN-ISO/IEC 17799:2003 Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.

Spełnienie wymogów praktycznych pozwoli na zapewnienie bezpieczeństwa przetwarzania danych o podwyższonym priorytecie (takie jak np.: dane finansowe i niejawne, dane osobowe wrażliwe).

Celem przedstawionej polityki bezpieczeństwa jest wskazanie działań, jakie należy wykonać oraz ustanowić zasady i reguły postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

1.1. Definicje używane w dalszej części niniejszego opracowania.

– **Dane Osobowe** (DO). Zgodnie z art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), za **dane osobowe** uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 2 ustawy). Stosownie do ust. 3 powołanego przepisu, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań. Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Daną osobową będzie taka informacja, która pozwala na ustalenie tożsamości danej osoby, bez nadzwyczajnego wysiłku i nakładów, zwłaszcza przy wykorzystaniu łatwo osiągalnych i powszechnie dostępnych źródeł. Poza zakresem przedmiotowej definicji znajdzie się zatem taka informacja, na podstawie której identyfikacja osoby wymagać będzie nieracjonalnych, nieproporcjonalnie dużych nakładów kosztów, czasu lub działań.
– **Przetwarzanie danych osobowych** oznacza jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
– **Administrator Danych Osobowych** (ADO) – Uniwersytet Warszawski rozumiany w sposób zgodny z ustawą o ochronie danych osobowych.
– **Administrator Bezpieczeństwa Informacji** (ABI) – osoba odpowiedzialna za dane ochronę danych osobowych w uczelni w sposób zgodny z ustawą o ochronie danych osobowych.
– **Lokalny Administrator Danych Osobowych** (LABI) – osoba odpowiedzialna za dane osobowe w wydzielonej jednostce lub grupie jednostek

1.2. Struktura organizacyjna.

W ramach struktury organizacyjnej uczelni, obowiązki ADO w zakresie ustawy o ochronie danych osobowych, zostały powierzone Kanclerzowi ds. Informatycznych, który jednocześnie pełni funkcję Administratora Bezpieczeństwa Informacji Uczelni.

Na wniosek Kierowników jednostek organizacyjnych ABI powołuje Lokalnych Administratorów Bezpieczeństwa Informacji LABI.

W administracji centralnej poszczególne Biura mogą powołać LABI, jednakże nadzór centralny w zakresie bezpieczeństwa pełni osoba powołana przez ABI w porozumieniu z Kanclerzem UW.

LABI mogą powołać Administratorów systemu w jednostce.

Schemat struktury organizacyjnej, oraz informacje o powołanych LABI znajdują się na stronie internetowej www.it.adm.uw.edu.pl

1.3. Zasady, standardy, wymagania polityki bezpieczeństwa.

1.3.1. Utworzenie lub zmiana ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów.

Kierownik jednostki wypełnia i podpisuje wniosek (formularz nr 4) o udzielenie pracownikowi dostępu do przetwarzania danych osobowych, który przekazuje do LABI, wraz z podpisanym przez pracownika oświadczeniem o ochronie danych osobowych.

LABI po podpisaniu wniosku, upoważnia (formularz nr 5) pracownika do przetwarzania danych osobowych zgodnie z Instrukcją i przekazuje upoważnienie administratorowi systemu informatycznego lokalnego lub administratorowi aplikacji centralnej (HMS, USOS, serwer pocztowy ADM, APD – DAK lub DSK)

LABI lub wyznaczona osoba w jego imieniu prowadzi ewidencję osób upoważnionych.

O wszelkich modyfikacjach uprawnień decyduje kierownik jednostki w porozumieniu z lokalnym LABI.

Kierownik jednostki powinien zadbać o to, aby stanowisko pracy nowego pracownika zatrudnionego przy przetwarzaniu danych osobowych znajdowało się w obszarze przetwarzania danych osobowych, (jeśli zachodzi konieczność należy zwiększyć obszar przetwarzania danych osobowych spełniając wymagania dotyczące tego obszaru).

1.3.2. Zgłoszenie lub modyfikacja informacji o nowym systemie informatycznym służącym do przetwarzania danych osobowych.

W celu zgłoszenia nowego systemu służącego do przetwarzania danych osobowych, lub modyfikacji istniejącego systemu, LABI lub wyznaczeni administratorzy systemów są zobligowani do przygotowania szczegółowej instrukcji zarządzania systemem informatycznym.

Instrukcje dotyczące systemów informatycznych funkcjonujących w jednostkach wymagają zatwierdzenia przez LABI.

Instrukcje zarządzania systemami informatycznymi ogólnouniwersyteckimi HMS, USOS, IRK, IRKBWZ, przygotowują administratorzy tych aplikacji. Instrukcje te zatwierdza ABI.

Zatwierdzone instrukcje stanowią obowiązujące dokumenty do stosowania.

Zawarte w niej procedury i wytyczne powinny być przekazane osobom odpowiedzialnym w jednostce za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności.

1.3.3. Definicja bezpieczeństwa informacji.

Bezpieczeństwo przetwarzania informacji jest kluczowym zadaniem w instytucjach przetwarzających dane w zespołach wieloosobowych takich jak Uniwersytet Warszawski. Celem bezpieczeństwa przetwarzania informacji jest zapewnienie możliwości współużytkowania informacji (w szczególności danych osobowych) w sposób zapewniający ich dostępność, poufność i integralność.

- **Dostępność** – cecha zapewniająca, że zasoby informacyjne są dostępne użytkownikowi w wymaganym miejscu, czasie i w wymaganej formie;
- **Poufność** – cecha zapewniająca, że dostęp do zasobów informacyjnych jest ograniczony tylko do kręgu osób uprawnionych.
- **Integralność** – cecha zapewniająca, że oryginalna forma lub stan zasobów może być zmieniony tylko przez osoby do tego uprawnione.

1.3.4. Wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa.

Poprawne wprowadzenie polityki bezpieczeństwa nie ogranicza się jedynie do wprowadzenia i zabezpieczenia urządzeń i pomieszczeń. Szkolenia dotyczące obowiązków pracowników przeprowadzone we wszystkich jednostkach Uniwersytetu Warszawskiego pozwolą na zwiększenie bezpieczeństwa danych. Zakres szkoleń, oraz merytoryczny nadzór nad szkoleniami w dziedzinie bezpieczeństwa danych należy do ABI.

1.3.5. Zapobieganie i wykrywanie wirusów i innego złośliwego oprogramowania.

W celu ochrony przed oprogramowaniem niepożądanym należy stosować dwa poziomy zabezpieczeń:

– **Zabezpieczenie pierwszego stopnia**: obejmujące zabezpieczenie poczty elektronicznej, oraz innych usług umożliwiających przesyłanie plików przed przesyłaniem oprogramowania niepożądanego. W tym celu serwery pocztowe, oraz serwery umożliwiające transfer plików powinny być zabezpieczone systemem antywirusowym Nie dopuszcza się doręczenia poczty zainfekowanej wirusami lub innym oprogramowaniem uznawanym za złośliwe rozpoznawanymi przez program antywirusowy. Obowiązek aktualizacji baz antywirusowych nakłada się na administratora serwera. Aktualizacja oprogramowania antywirusowego nie powinna odbywać się rzadziej, niż raz w tygodniu (nie rzadziej niż raz na trzy dni w przypadku, gdy aktualizacja odbywa się automatycznie).
– **Zabezpieczenie drugiego stopnia**: obejmujące zabezpieczeniem wszystkie komputery przetwarzające dane wrażliwe obejmujące instalację i aktualizację oprogramowania skanującego lokalny system w poszukiwaniu oprogramowania złośliwego.
  Polityka bezpieczeństwa nakłada obowiązek używania systemów antywirusowych zalecanych przez Pion Informatyczny UW. Oprogramowanie antywirusowe jest kupowane w ramach przetargu ogólnouniwersyteckiego. Więcej informacji na ten temat należy szukać na stronach: www.it.adm.uw.edu.pl
  Przestrzeganie zasad bezpieczeństwa sieci LAN zawiera załącznik nr 4.

1.3.6. Dbałość o ciągłość działania systemów.

Polityka bezpieczeństwa zaleca, aby kluczowe urządzenia były zasilane, z co najmniej dwóch niezależnych źródeł zasilania, oraz podłączone do urządzeń podtrzymujących napięcie (UPS). Serwisowanie urządzeń i sprzętu związanego z bezpieczeństwem przetwarzania informacji powinno następować w możliwie krótkim czasie od wykrycia jego awarii. Szybkie przywrócenie właściwego stanu technicznego urządzeń ma na celu wyeliminowanie z użycia sprzętu, który nie spełnia parametrów określonych przez szczegółowe instrukcje dotyczące elementów systemu przetwarzania danych osobowych. W szczególności oznacza to, iż nie jest dopuszczalne rezygnowanie z zabezpieczeń z powodu ich wadliwego działania spowodowanego awarią (np. pominięcie firewalla z powodu uszkodzenia). W czasie, gdy sprzęt przebywa w serwisie administrator powinien zapewnić sprzęt o właściwościach identycznych lub przewyższających go funkcjonalnością. Może w tym celu zastosować urządzenia mniej ważnej części podległej sieci, lub może zwrócić się do jednostki nadrzędnej o użyczenie sprzętu na czas usunięcia awarii.

1.3.7. Definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania przypadków naruszenia bezpieczeństwa.

Administratorzy systemów informatycznych odpowiedzialni są za bezpieczeństwo systemów w swojej jednostce organizacyjnej. Użytkownicy systemów informatycznych zobowiązani są do zastosowania się do wszystkich wskazówek i uwag administratora (w tym do respektowania nakazów i zakazów nałożonych przez administratora w zakresie użytkowania systemów informatycznych). Za bezpieczeństwo danych osobowych przetwarzanych w sposób tradycyjny odpowiada LABI.

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych w Uniwersytecie Warszawskim ujęta jest w Załączniku nr 3.

1.4. Bezpieczeństwo zbiorów danych osobowych przetwarzanych w sposób tradycyjny.

Zbiory danych osobowych przetwarzanych w sposób tradycyjny (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne) podlegają również ochronie na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Ewidencja, na którą składają się: wykaz budynków, pomieszczeń i części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe podlega obowiązkowi ewidencjonowania, a odpowiedzialnych za aktualność danych wyznacza się LABI.

Ewidencja ta zawiera również:

- Wykaz zbiorów danych osobowych przetwarzanych w sposób tradycyjny,
- Opis struktury zbiorów danych,
- Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności,
- Ewidencja osób uprawnionych.

Obszar, w którym przetwarzane są dane osobowe zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne za zgodą administratora danych, lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

Stanowisko pracy osoby przetwarzającej dane osobowe musi być ustawione w ten sposób, aby uniemożliwić nieupoważnionym osobom przebywającym w pomieszczeniu przeglądanie tychże informacji.

Zabrania się wynoszenia dokumentów, wydruków komputerowych, kartotek, oraz innych zbiorów danych poza obszar, w którym przetwarzane są dane osobowe.

2. Bezpieczeństwo systemów informatycznych.

2.1. Identyfikacja zasobów, określenie miejsca i sposobu ich przechowywania.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

Prowadzenie ewidencji danych dotyczących wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane wrażliwe należy do obowiązków LABI. Aktualizacja dokumentacji polega na wypełnieniu formularza nr 2.

Obszar, w którym przetwarzane są dane osobowe, powinno obejmować zarówno miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco). Zgodnie z treścią § 4 pkt 1, wskazanie miejsca przetwarzania danych osobowych powinno być określone poprzez określenie budynków, pomieszczeń lub części pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Do obszaru przetwarzania danych należy zaliczyć również pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, uszkodzone komputery i inne urządzenia z nośnikami zawierającymi dane osobowe). Do obszaru przetwarzania danych osobowych administrator danych powinien zaliczyć również miejsce w sejfie bankowym, archiwum, itp. jeśli wykorzystywane są one np. do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym, czy też do składowania innych nośników danych, np. dokumentów źródłowych.

Pomieszczenia należy zabezpieczyć przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

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

LABI są zobligowani do ewidencji danych dotyczących nazwy zbiorów danych, oraz stosowanych nazw używanych do ich przetwarzania programów komputerowych. W wykazie należy podać informacje w zakresie precyzyjnej lokalizacji miejsca (budynek, pomieszczenie, nazwa komputera lub innego urządzenia), w którym znajdują się zbiory danych osobowych formularz nr 1.

2.2.1. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Każdy z systemów informatycznych funkcjonujących na Uniwersytecie Warszawskim powinien posiadać dokumentację techniczną dostarczoną przez jego twórców. Dokumentacja tego typu powinna spełniać wymagania dotyczące struktur baz danych oraz funkcjonalności zarządzających nimi aplikacji zgodne z ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j. Dz.U. z 2002 r. Nr 101, poz. 926, późn. zm.). Dla nowych systemów informatycznych wymaganie to sprawdzane jest podczas testów akceptacyjnych przed dopuszczeniem aplikacji do użytku.

Dla każdego zidentyfikowanego zbioru danych należy podać opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane. Opis pola danych, w przypadkach, gdy możliwa jest niejednoznaczna interpretacja jego zawartości, powinien wskazywać nie tylko kategorię danych, ale również format jej zapisu i/lub określone w danym kontekście znaczenie.

2.2.2. Sposób przepływu danych pomiędzy poszczególnymi systemami.

Sposób przepływu danych pomiędzy poszczególnymi systemami powinien zostać opisany w dokumentacji technicznej tych systemów, lub w dokumentacji technicznej połączenia systemów.

Należy zamieścić również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych) lub półautomatycznie – za pomocą teletransmisji (przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu, np. wysyłka plików do ZUS. Dla identyfikacji procesów przetwarzania danych osobowych szczególne znaczenie ma specyfikacja przepływu danych w systemach z rozproszonymi bazami danych. W rozproszonej bazie danych, dane zlokalizowane są w różnych miejscach oddalonych od siebie terytorialnie i mogą zawierać, w zależności od lokalizacji, różne zakresy danych. Należy wskazać zakres przesyłanych danych, podmiotu lub kategorii podmiotów, do których dane są przekazywane oraz ogólnych informacji na temat sposobu przesyłania danych (Internet, poczta elektroniczna, inne rozwiązania), które mogą decydować o rodzaju narzędzi niezbędnych do zapewnienia ich bezpieczeństwa podczas teletransmisji.

2.2.3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

Systemy informatyczne eksploatowane na Uniwersytecie Warszawskim powinny być wyposażone w mechanizmy zapewniające:

– Ochronę i kontrolę dostępu do aplikacji użytkowych,
– Analizę modyfikacji danych,
– Kontrolę błędów wprowadzanych danych,
– Analizę poprawności przesyłanych danych.

Użytkownicy systemów informatycznych powinni zostać przeszkoleni przed rozpoczęciem pracy w systemie. Identyfikatory i hasła (lub inne środki uwierzytelniania) powinny być przekazane w formie zapewniającej poufność.

Każdy z systemów informatycznych powinien używać metod kryptograficznych podczas autoryzacji użytkowników, oraz zapewniać odpowiednio wysoki poziom bezpieczeństwa transmisji i przetwarzania danych.

2.3. Zasady nadawania, zmiany, zawieszania, przywracania i odwoływania uprawnień dostępu do systemów informatycznych zawierających dane osobowe.

2.3.1. Postanowienia ogólne.

W celu zapewnienia wymaganego poziomu bezpieczeństwa wszystkich systemów informatycznych należy zdefiniować minimalne wymagania dotyczące procedury kontroli uprawnień. Kontrolą ewidencji użytkowników w systemach informatycznych zajmują się LABI, oraz wyznaczeni przez nich administratorzy systemów. Szczegółowe postanowienia dotyczące każdego z systemów informatycznych muszą być zawarte się w instrukcjach szczegółowych. Dokumentację dotyczącą przetwarzania danych osobowych przetwarzanych przez system informatyczny tworzy i nadzoruje jej przestrzeganie LABI.

2.3.2. Klasy użytkowników.

Polityka bezpieczeństwa nakłada na każdy system komputerowy obowiązek utworzenia, co najmniej dwóch klas użytkowników:

– **Administratorzy** – użytkownicy zarządzający systemem informatycznym upoważnieni do nadawania praw dostępu do systemu użytkownikom na minimalnym poziomie umożliwiającym wykonanie powierzonych obowiązków.
– **Użytkownicy** - pozostali użytkownicy systemu informatycznego, którzy uzyskali uprawnienia do korzystania z systemu.

2.3.2.1. Procedura nadawania uprawnień administratora.

Każdy z systemów informatycznych Uniwersytetu Warszawskiego powinien posiadać przynajmniej jednego administratora systemów informatycznych, a w przypadku systemów o charakterze ogólnouniwersyteckim, co najmniej dwóch administratorów.

Uprawnienia na poziomie administratora aplikacji lokalnej można nadawać jedynie na podstawie pisemnego upoważnienia kierownika jednostki oraz LABI, natomiast upoważnienie dla administratorów systemów centralnych może być nadawane tylko przez ABI na wniosek kierownika jednostki.

Administrator systemu informatycznego zawierającego dane osobowe powinien być pracownikiem Uniwersytetu Warszawskiego przeszkolonym w zakresie bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych.

W przypadku, gdy do uwierzytelniania administratora używa się hasła, składa się ono, z co najmniej osiem znaków, zawiera małe i wielkie litery, oraz cyfry lub znaki specjalne.

W przypadku, gdy do uwierzytelniania używa się innych systemów (biometria, autoryzacja na podstawie kart magnetycznych, kluczy elektronicznych) wymagane jest spełnienie wszystkich wymagań producenta systemu uwierzytelniania zawartych w instrukcji i dokumentacji technicznej danego systemu.

Administrator powinien zabezpieczyć dostęp zdalny na konta uprzywilejowane (root, Administrator, itd.).

Administrator zobowiązany jest zabezpieczyć system informatyczny przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych, lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

Administrator stosuje środki kryptograficznej ochrony danych wykorzystywanych do uwierzytelniania.

2.3.2.2. Procedura nadawania uprawnień pozostałych użytkowników systemu.

– O imienne upoważnienie osób mających posiadać dostęp do danych osobowych, zwracają się Kierownicy jednostek, w których dane są przetwarzane.
– Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby posiadające upoważnienia LABI formularz nr 5.

Upoważnienie lokalnego administratora danych osobowych w sprawie nadania uprawnień do przetwarzania danych jest przekazywana do wiadomości:

– Wnioskodawcy,
– ABI,
– Administratora systemu informatycznego.

Osoba, która została po raz pierwszy upoważniona do przetwarzania danych osobowych podpisuje oświadczenie o zapoznaniu się z przepisami o ochronie danych osobowych – dostępne również na stronie www.it.adm.uw.edu.pl

Każda zmiana zakresu obowiązków osoby upoważnionej do przetwarzania danych powodująca konieczność zmiany uprawnień (roli) w systemie informatycznym jest zgłaszana pisemnie administratorowi systemu przez przełożonego osoby przetwarzającej dane osobowe.

Użytkownik nie logujący się do systemu informatycznego przez okres dłuższy, niż jeden miesiąc powinien posiadać zablokowane konto przez administratora systemu.

2.3.3. Zasady posługiwania się identyfikatorami i hasłami w systemach informatycznych zawierających dane osobowe.

Hasło musi składać się, z co najmniej ośmiu znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

Zabronione jest ujawnianie identyfikatorów lub haseł do systemów informatycznych przetwarzających dane wrażliwe (nawet w przypadku, gdy prosi o to osoba podająca się za administratora systemu, lub przełożonego itp.).

Zabronione jest stosowanie haseł, które w prosty sposób kojarzą się z danymi użytkownika, (np. imię, nazwisko, imiona dzieci, numer rejestracyjny pojazdu).

2.3.4. Kontrola praw dostępu do systemów informatycznych zawierających dane osobowe.

Osoba, która otrzymała upoważnienie do przetwarzania danych osobowych, nazywana użytkownikiem systemu, zgłasza się do administratora systemu informatycznego w celu uzyskania identyfikatora oraz hasła.
Administrator systemu informatycznego rejestrujący uprawnienia do przetwarzania danych tworzy dla użytkownika systemu:

- Jednoznaczny i niepowtarzalny identyfikator logowania do serwera,
- Jednorazowe hasło dostępu do systemu informatycznego, które użytkownik powinien zmienić z chwilą zalogowania się systemu.
- Zestaw uprawnień umożliwiający dostęp do przetwarzania danych zgodnie z zakresem obowiązków służbowych pełnionych przez osobę lub zgodnie z podanymi uprawnieniami na Formularzu udostępnionym jednostkom i podpisanymi przez kierownika jednostki oraz LABI.
- Administrator przekazuje identyfikator i hasło jednorazowe podczas pierwszego krótkiego szkolenia osobiście,
- W trakcie pierwszego logowania do systemu, system powinien wymuszać zmianę hasła.
- Administrator zna hasło użytkownika tylko w momencie jego nadawania.
- Użytkownik w przypadku braku aktywności przez jedną godzinę zostaje automatycznie wylogowany z systemu (dotyczy to przede wszystkim systemów o znaczeniu ogólnouczelnianym).
- Użytkownik, który zapomniał hasła musi zgłosić się do administratora o nadanie nowego.

2.3.5. Wdrożenia kolejnych wersji systemów informatycznych zawierających dane osobowe.

Administrator systemu informatycznego zobowiązany jest do stworzenia systemu dystrybucji i aktualizacji wersji oprogramowania, oraz utworzenia instrukcji aktualizacji.

2.3.6. Zasady i tryb nadawania, zmiany, odwołania oraz zawieszenia i przywracania praw dostępu do pomieszczeń i urządzeń umożliwiających dostęp do systemów informatycznych zawierających dane osobowe.

Przez bezpośredni dostęp do systemu informatycznego rozumie się dostęp bez użycia dodatkowych metod autoryzacji (np. dostęp do plików baz danych).

Tylko administratorzy systemu informatycznego mają bezpośredni dostęp do systemów informatycznych zawierających dane osobowe.

Załącznik nr 2
do zarządzenia nr 39 Rektora UW z dnia 15 listopada 2007 r.
w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH ZE SZCZEGÓLNYM UWZGLĘDNIENIEM WYMOGÓW BEZPIECZEŃSTWA INFORMACJI.

Niniejsza instrukcja określa ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych na Uniwersytecie Warszawskim oraz stanowi podstawę do opracowania szczegółowych instrukcji dla każdego z użytkowanych systemów.

1. Zasady i procedury nadawania uprawnień do przetwarzania danych osobowych.

Przy opracowywaniu instrukcji szczegółowej dla każdego systemu należy szczegółowo opisać:

- Procedury przyznawania/usuwania użytkownikowi identyfikatora w systemie informatycznym.
- Tryb nadawania identyfikatorów i haseł (łącznie z określeniem ich długości, przyjętej struktury i stopnia złożoności). Częstotliwość zmiany hasła (hasło powinno być zmieniane nie rzadziej, niż co 30 dni oraz powinno zawierać kombinację liter i cyfr).
- Procedury nadawania, modyfikacji i usuwania uprawnień do zasobów systemu informatycznego.
- Procedury rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.
- Sposób przechowywania haseł administratorów lub dokładny opis innych metod autoryzacji.
- Zasady administrowania systemem informatycznym w przypadkach awaryjnych (braku administratora).
- Procedury przekazywania uprawnień na czas planowanej nieobecności administratorów (urlopy).

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

- Formy przekazywania haseł użytkownikom (pisemna, ustna, inna).
- Wskazanie osób odpowiedzialnych za przydział haseł.
- Inne stosowane metody weryfikacji tożsamości użytkownika (poza konto i hasło).

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

- Wykaz czynności, jakie musi wykonać użytkownik w celu uruchomienia systemu informatycznego.
- Wykaz czynności, jakie musi wykonać użytkownik w celu zamknięcia dostępu do systemu informatycznego.
- Wykaz czynności, jakie musi wykonać użytkownik w celu tymczasowego zaprzestania pracy w systemie informatycznym.

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

- Metody i częstotliwość tworzenia kopii zapasowych danych oraz kopii zapasowych systemu informatycznego używanego do ich przetwarzania.
- Zakres danych dla jakich będą wykonywane kopie zapasowe.
- Typ nośników oraz narzędzia programowe i urządzenia, które mają być do tego celu wykorzystane.
- Harmonogram wykonywania kopii.
- Procedury likwidacji/utylizacji nośników zawierających dane wrażliwe w tym dyskietki, CD i inne.
- Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków (dodatkowe urządzenia, budynki).
- Procedury niszczenia papierowych nośników informacji (niszczarki).

5. Sposób, miejsce i okres przechowywania kopii zapasowych.

- Miejsce, sposób i czas przechowywania wszelkiego rodzaju nośników zawierających kopie bezpieczeństwa danych osobowych.
- Sposób zabezpieczenia tych nośników przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
- Metody i częstotliwość wykonywania kopii awaryjnych.
- Archiwizacja systemu

6. Sposoby zabezpieczenia systemu informatycznego.

- Metody i częstotliwość sprawdzania systemów informatycznych na obecność wirusów komputerowych oraz metod ich usuwania
- Określenie stosowanych standardów w zakresie oprogramowania antywirusowego (standardy ogólnouniwersyteckie, lokalne) – stacje robocze, serwery
- Opis obszarów systemu informatycznego narażone na ingerencję wirusów komputerowych i innego oprogramowania szkodliwego.
- Procedury postępowania w przypadku, gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia.
- Procedury reakcji na zagrożenie z sieci publicznej.
- Procedury dostępu do pomieszczeń i komputerów, w których są przetwarzane dane osobowe
- Procedury fizycznego i logicznego zabezpieczenia komputerów biorących udział w przetwarzaniu danych osobowych.
- Procedury ochrony danych przed utratą z powodu zakłóceń lub awarii sieci zasilania.

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

System informatyczny powinien zapewnić odnotowanie informacji o udostępnieniach danych odbiorcom w rozumieniu art. 7 pkt 6 ustawy, zawierające informacje komu, kiedy, i w jakim zakresie dane osobowe zostały udostępnione, chyba, że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

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

- Cel, zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji systemu informatycznego. Należy wskazać podmioty i osoby uprawnione do dokonywania przeglądów i konserwacji systemu informatycznego.
- Zasady przekazywania nośników elektronicznych do naprawy uniemożliwiające odczytanie wcześniejszych zapisów na nich danych osobowych: wcześniejsze kasowanie danych, pod nadzorem administratora aplikacji.

Załącznik nr 3
do zarządzenia nr 39 Rektora UW z dnia 15 listopada 2007 r.
w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH NA UNIWERSYTECIE WARSZAWSKIM

§ 1

Instrukcja niniejsza ma zastosowanie w sytuacjach:
1) stwierdzonego naruszenia zabezpieczenia (ew. ochrony) danych osobowych w systemie informatycznym lub innym zbiorze danych;
2) podejrzenia naruszenia zabezpieczenia (ew. ochrony) danych osobowych w systemie informatycznym lub innym zbiorze danych.

§ 2

Naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych stwierdza się, gdy wystąpiły między innymi:
1) nieuprawniony dostęp do danych osobowych;
2) udostępnienie danych osobowych osobom nieupoważnionym;
3) zmiany, kopiowanie lub uszkodzenie danych osobowych dokonane przez osoby nieuprawnione;
4) kradzież nośników informacji zawierających dane osobowe (np. dysków, dyskietek, płyt CD, płyt DVD, wydruków komputerowych).

§ 3

Za okoliczności, które wskazują na naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych, uważa się między innymi:
1) nieuzasadnione korzystanie z zasobów systemu informatycznego lub innego zbioru danych;
2) nieuzasadnione ujawnienie danych osobowych;
3) ujawnienie wirusów komputerowych lub innych programów, które mogą mieć negatywny wpływ na funkcjonowanie systemu informatycznego;
4) wydarzenia obniżające stan bezpieczeństwa systemu informatycznego lub innego zbioru danych (np. awaria zasilania).

§ 4

Osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym lub innym zbiorze danych, która stwierdzi lub podejrzewa naruszenie zabezpieczenia danych zobowiązana jest do:
1) niezwłocznego poinformowania o tym fakcie LABI i swojego bezpośredniego przełożonego,
2) zaprzestania pracy w systemie informatycznym lub innym zbiorze danych do momentu otrzymania od LABI decyzji o możliwości wznowienia pracy.

§ 5

1. LABI po uzyskaniu informacji, o której mowa §4 zawiadamia o naruszeniu zabezpieczenia danych osobowych ABI Uniwersytetu Warszawskiego i bezpośredniego przełożonego oraz podejmuje działania w celu rozpoznania naruszenia zabezpieczenia danych, a w szczególności ustala, czy miało miejsce naruszenie ochrony danych osobowych, a w sytuacji nie potwierdzenia podejrzeń wydaje decyzję, o której mowa w § 4 ust.1 pkt 2 oraz sporządza i przedstawia w ciągu 14 dni ABI UW raport o podejrzeniu naruszenia ochrony danych osobowych w systemie informatycznym lub innym zbiorze danych.
2. ABI w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych:
1) podejmuje działania służące ograniczeniu szkód wywołanych naruszeniem ochrony danych osobowych;
2) zabezpiecza dane wskazujące na naruszenie zabezpieczenia danych osobowych;
3) ustala okoliczności naruszenia ochrony danych osobowych;
4) analizuje rodzaj, zakres i źródło naruszenia ochrony danych osobowych;
5) podejmuje działania naprawcze;
6) bada przyczyny naruszenia ochrony danych osobowych i podejmuje działania mające na celu wyeliminowanie podobnych zdarzeń zagrażających bezpieczeństwu danych.

§ 6

ABI, po czynnościach, o których mowa w § 5, sporządza i przedstawia ADO UW raport o stwierdzeniu naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych w ciągu 14 dni od daty jego zaistnienia. Raport zawiera w szczególności następujące dane i informacje:

1) imię i nazwisko, stanowisko osoby, która zgłosiła naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych;
2) miejsce zatrudnienia osoby, o której mowa w pkt 1;
3) datę i godzinę powiadomienia o naruszeniu;
4) opis podjętych działań mających na celu ustalenie zakresu podejrzewanego naruszenia;
5) opis podjętych działań naprawczych.

§ 7

1. Lokalny Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przechowywanie materiałów, o których mowa § 5, dokumentujących zaistniałe naruszenie oraz podejrzenie naruszenia zabezpieczenia danych w systemie informatycznym lub innym zbiorze danych.

2. Zgłoszenie przypadków naruszenia bezpieczeństwa odbywa się w następujący sposób na wszystkich poziomach uprawnień:

1) Zgłoszenie przypadku naruszenia bezpieczeństwa należy zgłosić przełożonemu, administratorowi oraz LABI właściwemu dla danej jednostki organizacyjnej,
2) Jeśli skutki oraz przyczyny naruszenia polityki bezpieczeństwa nie są możliwe do usunięcia przez LABI zgłasza się on o pomoc do jednostki nadrzędnej (w przypadku, gdy brak takiej jednostki zgłoszenie powinno być kierowane do ABI,
3) Jednostka poinformowana o przypadku naruszenia bezpieczeństwa jest zobowiązana do usunięcia przyczyn naruszenia,
4) Zgłoszenie na każdym szczeblu musi być ewidencjonowane centralnie w systemie zgłaszania przypadków naruszenia bezpieczeństwa,
5) ABI powinien zgłaszać podległym jednostkom organizacyjnym przypadki naruszenia bezpieczeństwa oraz informować o potencjalnych możliwościach naruszenia polityki bezpieczeństwa.

Załącznik nr 4
do zarządzenia nr 39 Rektora UW z dnia 15 listopada 2007 r.
w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim

BEZPIECZEŃSTWO SIECI LAN/WLAN

1.1. Normy

Każdy nowy system okablowania strukturalnego musi spełniać wymagania aktualnie obowiązujących norm: ISO/IEC 11801:2002 wydanie drugie lub EN 50173-1:2002 wydanie drugie, dotyczących okablowania strukturalnego budynków.

Wymagane jest również dołączenie do dokumentacji odpowiednich certyfikatów zgodności komponentów i systemu okablowania z jednym z obowiązujących standardów:

1) ISO/IEC 11801:2002 wydanie drugie
2) EN50173-1:2002 wydanie drugie
3) ANSI/TIA/EIA 568-B.2 Cat.6
4) draft specyfikacji JTC 1/25N 981

W przypadku, gdy zachodzi potrzeba uzupełnienia okablowania istniejącej sieci kategorii 5e dopuszcza się stosowanie okablowania kategorii 5e.

1.2. Okablowanie

Całość budynku powinna posiadać okablowanie strukturalne, co najmniej kategorii 6 z podziałem na okablowanie pionowe i poziome integrujące wszystkie systemy teletechniczne włącznie z siecią telefoniczną instalowane w budynku oraz dedykowaną sieć energetyczną do zasilania lokalnej sieci komputerowej.

Wydajność okablowania powinna być zgodna z najnowszymi wytycznymi komitetów normalizacyjnych, tj. draftem specyfikacji JTC 1/25N 981 określającym pasmo przenoszenia dla systemów Klasy E/Kategorii 6 na 625MHz, a pasmo przenoszenia dla systemów Klasy F/Kategorii 7 na 1GHz.

Trasy prowadzenia przewodów transmisyjnych okablowania poziomego oraz kabli okablowania pionowego należy skoordynować z istniejącymi i wykonywanymi instalacjami w budynku m.in. dedykowaną instalacją elektryczną, instalacją elektryczną ogólną, instalacją centralnego ogrzewania, wody, gazu, itp.

1.2.1. Poziome

Ze względu na bezpieczeństwo transmisji oraz w celu zminimalizowania oddziaływania zakłóceń, szczególnie w miejscach o dużej ilości kabli transmisyjnych i nakładania się różnych instalacji prądowych, w projekcie należy przewidzieć budowę okablowania poziomego w wersji ekranowanej lub światłowodowej. Spełnienie postulatów kompatybilności elektromagnetycznej, a więc zwiększenie odporności systemu informatycznego na zakłócenia elektromagnetyczne oraz ograniczenie emisji zakłóceń do środowiska zewnętrznego znacząco zwiększa bezpieczeństwo transmisji danych.

1.2.2. Pionowe

Kanały na instalację pionową powinny być odpowiedniej przepustowości. Zabrania się tworzenia rozwiązań doraźnych służących jedynie do wykonania bieżącej inwestycji.

1.2.3. Międzywęzłowe

Wskazane jest stosowanie światłowodów do połączeń międzywęzłowych.

1.3. Zasilanie energetyczne

Tam, gdzie to możliwe proponuje się zastosowanie POE. Docelowo wszystkie urządzenia powinny pracować w tym systemie.

Sieć zasilająca infrastrukturę techniczną systemu informatycznego musi być wykonana w postaci wydzielonej instalacji elektrycznej oraz mieć możliwość podtrzymywania napięcia w sytuacjach awaryjnych pozwalających na bezpieczne wyłączenie urządzeń.

W tym celu należy stworzyć oddzielnie dwie instalacje:

1.3.1. Dedykowane dla komputerów

Instalacja oznaczona kolorem czerwonym przeznaczona do podłączania urządzeń sieciowych i sprzętu komputerowego. Instalacja ta powinna być wyposażona w system zasilania awaryjnego umożliwiającego w sytuacjach awaryjnych na bezpieczne wyłączenie urządzeń. Nie można do tej instalacji podłączać innych urządzeń, niż komputery, monitory, urządzenia sieciowe.

1.3.2. Niededykowane

Instalacja oznaczona kolorem białym, do której nie należy podłączać urządzeń sieciowych i sprzętu komputerowego (jest przeznaczona do zasilania pozostałych urządzeń elektrycznych).

1.3.3. UPS

Czas podtrzymania zasilania pracy urządzeń aktywnych powinien być obliczony w taki sposób, by było możliwe bezpieczne wyłączenie zasilanych urządzeń aktywnych w przypadku zaniku zasilania w sieci. Na potrzeby doboru typu i producenta UPS, należy wstępnie oszacować maksymalną i nominalną moc [kVA] urządzenia podtrzymującego zasilanie w oparciu o sumaryczny pobór mocy zasilanych urządzeń.

Moc przewidziana na standardowe pojedyncze gniazdo zasilania PC powinna wynosić ok. 200÷300 [W], dla drukarki laserowej ok. 1 [kW]. Standardowo w jeden obwód prądowy zaleca się grupować ok. 10 gniazd.

1.4. PEL

W każdym pomieszczeniu użytkowników systemów specjalizowanych, jak również w pomieszczeniach biurowych powinny zostać zainstalowane punkty elektryczno – logiczne składające się z dwóch gniazd logicznych i 4 gniazd elektrycznych wg następującej zasady:

1) pokój jednoosobowy 2 PEL,
2) pokój dwuosobowy 3 PEL,
3) pokój 3 osobowy 4 PEL.

Wyjątek stanowią pomieszczenia techniczne serwerowni, pomieszczenie obsługi technicznej centrum monitoringu i zarządzania, pomieszczenie administratorów sieci lokalnej LAN i WLAN oraz sale uruchomień i testów sprzętu i oprogramowania, gdzie ilość PEL powinna być określana w zależności od potrzeb.

Przy projektowaniu sieci i montażu PEL należy uwzględnić zasady ergonomii w zakresie ich rozmieszczenia np. odległości od podłogi (30÷50 [cm] lub większej). W czasie eksploatacji, należy zadbać, aby do wydzielonych obwodów zasilania sieci komputerowej nie były podłączone inne urządzenia
np. czajniki, grzejniki itp. W przypadku, gdy istnieje konieczność poprowadzenia instalacji bezpośrednio na podłodze należy zastosować kanały PCV, które pozwolą zabezpieczyć okablowanie przed zniszczeniem.

1.5. Wymagania budowlane

W przypadku budowy sieci LAN w nowych budynkach wymagane są jedynie prace dostosowawcze konfiguracyjne zależnie od potrzeb. W przypadku budynków o starszej konstrukcji, czy też zabytkowych wymagane jest wcześniejsze rozpoznanie najdogodniejszych rozwiązań – trasowania okablowania lub też uzyskania stosownych zezwoleń dla budynków o charakterze zabytkowym. W przypadku starszych budynków okablowanie powinno być prowadzone w rynnach PCV lub w podwieszkach sufitowych wraz z pozostałym okablowaniem. Zalecana jest integracja sieci komputerowej, alarmowej, telewizyjnej, przeciwpożarowej, telefonicznej w postaci jednego okablowania strukturalnego (znaczne obniżenie kosztów – ułatwione zarządzanie, konfiguracja i rekonfiguracja sieci itp.).

Instalacje prowadzone w ścianach powinny być wykonane w gładkich rurach PCV. Rury powinny być prowadzone w liniach prostych, a tam, gdzie zmieniają kierunek muszą zostać zainstalowane drzwiczki rewizyjne.

1.6. Węzeł sieci

Węzły sieciowe powinny znajdować się w wydzielonych pomieszczeniach, do których dostęp powinny mieć jedynie osoby uprawnione (pracownicy Dział Sieci Komputerowych, ICM, pracownicy techniczni jednostki organizacyjnej).

Okablowanie węzła powinno spełniać podstawowe wymagania:

1) opis i numeracja gniazd w szafach krosowniczych i PEL'i powinna być wykonana w sposób jednoznaczny i nie nastręczać trudności w interpretacji zarówno w bieżącym użytkowaniu sieci jak i przy rozbudowie okablowania strukturalnego;
2) dla każdego piętra w budynku (lub segmentu sieci, lub piętra i segmentu sieci) powinna być przewidziana wydzielona szafa krosownicza;
3) kable łączące serwery i urządzenia z szafą krosowniczą lub też inne o istotnym znaczeniu powinny być w innym kolorze niż pozostałe i specjalnie numerowane – ułatwia to zarządzanie;
4) projekt powinien uwzględniać budowę okablowania w oparciu o kabel UTP kategorii 6, a także połączenie punktów dystrybucyjnych kablami optycznymi.
5) dedykowaną dla okablowania instalację elektryczną należy wykonać zgodnie z obowiązującymi normami i przepisami (minimalne wymagania elementów okablowania strukturalnego to kategoria 6 / klasa E oraz RJ45 jako interfejs końcowy dla połączeń na skrętce miedzianej 4 parowej).

1.6.1. Szafa

Zaleca się instalowanie szaf krosowniczych 19” stojących 42U lub wiszących podwójnie łamanych na poszczególnych piętrach budynku w wydzielonych pomieszczeniach. Należy zapewnić swobodny dostęp ze wszystkich stron do szafy.

1.6.2. Okablowanie

Okablowanie w węzłach powinno być rozmieszczone w sposób uporządkowany. Należy unikać splątania przewodów, a zapas kabla umieszczać poza szafą dystrybucyjną.

1.6.3. Urządzenia

Urządzenia aktywne sieci powinny umożliwiać zdalne zarządzanie. Zdalne zarządzanie powinno obsługiwać VLAN. W przypadku, gdy urządzenie ma być zastosowane w planowanej instalacji WLAN konieczne jest zastosowanie urządzeń POE.

1.6.4. Wentylacja/klimatyzacja

Pomieszczenia powinny być zabezpieczone przed dostępem osób nieupoważnionych i mieć zapewniony odpowiedni poziom wentylacji umożliwiający poprawną eksploatację zamontowanego tam sprzętu. W przypadku niewystarczającej samoistnej wentylacji i zbyt wolnej wymiany powietrza w pomieszczeniu należy stosować dodatkowe wentylatory lub wyposażyć obudowę szafy w dodatkowe otwory wentylacyjne.

Klimatyzacja węzła sieci powinna być dostosowana do warunków pomieszczenia i mocy cieplnej wydzielanej przez zainstalowane urządzenia.

Należy zapewnić również odpowiednią wentylację i klimatyzację pomieszczeń, w których zainstalowano aktywne urządzenia sieciowe (serwery, routery, UPS i inne). W pomieszczeniach tych należy sprawdzać poprawność instalacji systemu wentylacji jak też zapewnić okresowe kontrole i monitoring temperatury. Do pomieszczenia (pomieszczeń) UPS powinno być doprowadzone okablowanie logiczne, tak by istniała możliwość zdalnego monitorowania i zarządzania pracą UPS z pomieszczenia administratora. Pomieszczenia techniczne, w tym serwerownie powinny być zabezpieczone przed dostępem osób trzecich. Wszystkie elementy związane z systemem zasilania dedykowanego powinny być starannie oznakowane. Główne bezpieczniki, przełączniki, 'bypass', doprowadzenia w głównej szafie zbiorczej zasilania jak i poszczególne podziały na obwody prądowe, kolejność faz w głównym przyłączu powinny być jasno i prosto oznakowane zgodnie z dokumentacją.

1.6.5. Oświetlenie

Wymaga się zastosowania oświetlenia zapewniającego prawidłową widoczność szafy dystrybucyjnej ze wszystkich stron.

1.6.6. Pomieszczenie

Pomieszczenie przeznaczone na węzeł sieci powinno zapewnić swobodną obsługę szafy dystrybucyjnej i urządzeń (wokół szafy powinien być zapewniony co najmniej metr wolnego miejsca).

1.6.7. Dostęp do pomieszczenia

Dostęp do węzłów sieci ograniczony powinien zostać jedynie dla uprawnionego personelu technicznego jednostki organizacyjnej Uniwersytetu Warszawskiego, oraz pracowników jednostek odpowiedzialnych za szkielet sieci (ICM, Dział Sieci Komputerowych).

1.7. Serwerownia

Pomieszczenie techniczne serwerowni to główny punkt dystrybucyjny okablowania strukturalnego, w którym zbiegać się będzie okablowanie poziome i pionowe obiektu, kable światłowodowe, jak również doprowadzenia traktów sieci rozległej we/wy od głowicy telekomunikacyjnej budynku. Jako urządzenia aktywne można zastosować przełączniki zarządzalne warstwy 3, które powinny posiadać dożywotnią gwarancję producenta. Do połączenia okablowania szkieletowego sieci może być wykorzystany przełącznik światłowodowy w standardzie 1000Base-SX.

1.7.1. Szafa

Wszystkie urządzenia aktywne, pasywne, modemy i serwery powinny być umieszczone w szafach dystrybucyjnych typu „rack". Szafy krosownicze i teletechniczne powinny być montowane w standardzie 19" i umożliwiać zainstalowanie odpowiedniej liczby urządzeń aktywnych.

1.7.2. Okablowanie

O ile jest to możliwe w serwerowni zalecane jest stosowanie podłogi technologicznej , co w trakcie eksploatacji sieci ułatwi prowadzenie i rekonfigurację okablowania strukturalnego. Podłoga powinna być antystatyczna i niepalna ze względu na koncentrację w pomieszczeniu urządzeń pracujących w sposób ciągły. Liczba gniazd (punktów PEL) powinna być o 20% większa od wstępnie oszacowanej w serwerowni i pomieszczeniu administratorów.

1.7.3. Urządzenia

Liczba elementów aktywnych zależy od ilości punktów sieci. Należy przyjąć, że na każde 48 punktów logicznych należy przewidzieć miejsce w szafie o wysokości 2U. W szafach powinno być zarezerwowana przestrzeń umożliwiająca ewentualne ustawienie urządzeń teletransmisyjnych o wysokości 15 [cm]. Szafa powinna uwzględniać miejsce na zamontowanie lokalnego UPS'a podtrzymującego działanie urządzeń aktywnych zamontowanych w szafie. W szafie powinna być zainstalowana listwa zasilająca (lub listwy, w zależności od potrzeb) umożliwiająca zasilanie zamontowanych tam urządzeń.

Montowane w szafach koncentratory (HUB'y) i przełączniki (SWITCH'e) i urządzenia transmisji danych (ROUTER'y, MODEM'y), powinny pochodzić od renomowanych producentów i tak dobrane, by zabezpieczały około 5÷10 % wolnych gniazd dla łatwej rekonfiguracji połączeń w ramach sieci lokalnej. Zalecane jest zaimplementowanie zapasowego (redundantnego) łącza teletransmisyjnego.

Dla zabezpieczenia planowanej do wdrożenia korporacyjnej sieci WLAN w szafach teletechnicznych serwerowni należy przewidzieć miejsce do włączenia i uruchomienia dodatkowego routera i urządzenia bezpieczeństwa dostarczanych przez operatora telekomunikacyjnego (należy zwrócić uwagę na to, aby te urządzenia były zasilane w systemie POE).

1.7.4. UPS

UPS - serwerownia, o co najmniej mocy sumarycznej serwerów i urządzeń aktywnych obsługujących użytkowników poszczególnych aplikacji lub jednego centralnego UPS o mocy pozwalającej na podtrzymanie wszystkich urządzeń aktywnych komputerowej sieci lokalnej.

Dla kluczowych urządzeń (zapewniających dostęp do usług dla wielu jednostek) przewidziane są inne wymagania dotyczące zasilania opisane w dokumencie Zarządzanie bezpieczeństwem danych osobowych – Polityka bezpieczeństwa Uniwersytetu Warszawskiego.

1.7.5. Wentylacja/klimatyzacja

Klimatyzacja w pomieszczeniu serwerowni powinna być dostosowana do warunków pomieszczenia i mocy cieplnej wydzielanej przez zainstalowane urządzenia.

Zaleca się stosowanie klimatyzacji podłogowej doprowadzającej chłodzenie bezpośrednio do szaf dystrybucyjnych.

1.7.6. Oświetlenie

Wymaga się zastosowania oświetlenia zapewniającego prawidłową widoczność szafy dystrybucyjnej ze wszystkich stron.

1.7.7. Sejf na nośniki

Serwerownia powinna być wyposażona w szafę pancerną, zabezpieczoną ppoż. przeznaczoną do przechowywania zapasowych kopii danych oraz użytkowanych systemów i aplikacji, pakietów oprogramowania oraz innych informacji i danych podlegających szczególnej ochronie. Korzystnym jest, aby wszystkie pomieszczenia techniczne serwerowni były pomieszczeniami przyległymi i były ze sobą połączone.

1.7.8. Pomieszczenia

Systemy alarmowe przeciw włamaniowe i przeciw napadowe powinny spełniać wymagania trzeciego poziomu tzn. kategorii SA3 według PN-93/E-08390/14. Również zabezpieczenia ochrony fizycznej – budowlane i mechaniczne - powinny spełniać wymagania trzeciego poziomu. Czas ich pokonania z użyciem specjalistycznych narzędzi nie powinien być krótszy niż 8 min.

1.7.9. Dostęp do pomieszczenia

Serwerownia powinna być zabezpieczona przed dostępem osób trzecich z dodatkowymi zabezpieczeniami w zakresie ochrony przeciwpożarowej.
Pomieszczenie(a) przeznaczone dla administratorów oraz operatorów powinno być (o ile to możliwe) oddzielone fizycznie od pomieszczenia technicznego serwerowni.

1.8. Przyłącza do budynku

Połączenia pomiędzy budynkami powinny być wykonywane przy użyciu łącz światłowodowych (stosowanie łącz galwanicznych może powodować uszkodzenia urządzeń sieciowych podczas wyładowań atmosferycznych).
Przyłącza światłowodowe powinny znajdować się w miejscach, do których dostęp jest ograniczony.

Rozwojem i utrzymaniem sieci szkieletowej zajmuje się Dział Sieci ICM, oraz Dział Sieci Komputerowych (w zakresie sieci administracyjnej). Zadaniem jednostki organizacyjnej Uniwersytetu Warszawskiego jest dystrybucja sieci LAN i WLAN w ramach jednostki.

1.9. Testowanie i szkolenie

Poprawność wykonania instalacji sieci sygnałowej powinna być potwierdzona pomiarami statycznymi i dynamicznymi właściwości poszczególnych torów. Pomiary takie wykonuje się specjalistycznymi testerami okablowania (np. OmniScanner, DSP 4300). Należy przeprowadzić testy okablowania dla wszystkich punktów przyłączeniowych. Dla łączy światłowodowych należy przeprowadzić pomiary tłumienności zgodnie z wymaganiami odpowiednich standardów (dwukierunkowe pomiary sygnałem w dwóch oknach transmisyjnych). Wszystkie raporty z pomiarów powinny zostać dołączone do dokumentacji powykonawczej i przekazane zamawiającemu.

Szkolenia administratorów i użytkowników systemów w zakresie bezpieczeństwa – proces podnoszenia poziomu świadomości użytkowników oraz doskonalenia umiejętności bezpiecznej eksploatacji systemu, w tym postępowania w przypadku wystąpienia incydentów (naruszenia zasad) bezpieczeństwa lub sytuacji kryzysowych.

Zagrożenie: użytkownicy o niskim poziomie świadomości z zakresu bezpieczeństwa, poprzez nonszalanckie, lekkomyślne obchodzenie się z zasobami lub chaotycznie działający w sytuacji kryzysowej mogą znacznie obniżyć skuteczność systemu bezpieczeństwa użytkowanych aplikacji.
Polityka bezpieczeństwa: szkolenie powinno być elementem decydującym o stanie bezpieczeństwa aplikacji i funkcjonowania systemu informatycznego jednostki. Szkolenia powinny dotyczyć wszystkich użytkowników i administratorów sieci i systemu a także służb ochrony. Zakres i formy szkoleń powinny być dostosowane do zakresu obowiązków i odpowiedzialności poszczególnych pracowników i osób funkcyjnych.

Zabezpieczenia:

Pełnomocnik ochrony i administrator bezpieczeństwa powinni organizować systematyczne wewnętrzne szkolenia, testy i ćwiczenia dotyczące postępowania administratorów i użytkowników systemu informatycznego z zasobami informacyjnymi oraz postępowania w przypadku wystąpienia incydentów bezpieczeństwa lub sytuacji kryzysowych.

Wybrane właściwości systemu zabezpieczeń sieciowych typu firewall/AV:

System zabezpieczeń powinien realizować zadania firewall, wykonując kontrolę na poziomie sieci oraz aplikacji. Może to być rozwiązanie programowe lub sprzętowo − programowe. System zabezpieczeń musi umożliwiać wykrywanie i blokowanie ataków intruzów IDP (Intrusion Detection and Prevention), zarządzanie pasmem sieci (QoS) oraz posiadać możliwość zestawiania zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site.

System zabezpieczeń powinien posiadać wbudowany moduł kontroli antywirusowej umożliwiający kontrolę poczty elektronicznej (SMTP, POP3) oraz HTTP. Włączenie kontroli antywirusowej nie wymaga dodatkowego serwera. Aktualizacja bazy wirusów oraz sygnatur ataków in-line IDS (Deep Packet Inspection) powinna odbywać się na żądanie, bądź automatycznie zgodnie z zaplanowanym harmonogramem.

System zabezpieczeń powinien być oparty o dedykowane urządzenie sieciowe nie posiadające wrażliwych na awarie elementów sprzętowych (np. twardego dysku). System zabezpieczeń nie powinien posiadać ograniczeń na liczbę chronionych komputerów w sieci wewnętrznej. System zabezpieczeń firewall zgodnie z ustaloną polityką bezpieczeństwa powinien umożliwiać prowadzenie kontroli ruchu sieciowego pomiędzy dwoma obszarami sieci (strefami). Polityki bezpieczeństwa powinny być definiowane pomiędzy dowolnymi strefami.

Urządzenia zabezpieczeń powinny posiadać możliwość podłączenia modemu i automatycznego zestawiania łącza zapasowego Dialup w razie wystąpienia awarii łącza podstawowego. Polityka bezpieczeństwa systemu zabezpieczeń powinna uwzględniać strefy bezpieczeństwa, adresów IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ). System zabezpieczeń powinien umożliwiać administratorom wykrywanie i blokowanie technik i ataków stosowanych przez hakerów, ochronę sieci przed atakami powtórzeniowymi (Replay Attack) oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP.

Zarządzanie zabezpieczeniami w pełnym zakresie powinno odbywać się z linii poleceń (CLI) oraz graficznej konsoli GUI. W systemie musi istnieć możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy powinni być uwierzytelniani za pomocą haseł statycznych, haseł dynamicznych (RADIUS, RSA SecureID) oraz certyfikatów SSL.

1.10. Dokumentacja

Dokumentacja powinna być wykonana przez wykonawcę i powinna spełniać wymagania przewidziane w rozszerzonej wersji tego dokumentu (dostępnej w postaci załącznika).

Dokumentację projektową wykonania sieci LAN, WLAN należy konsultować z działami sieciowymi Uniwersytetu Warszawskiego (Dział Sieci ICM, Dział Sieci Komputerowych). Realizacja inwestycji wymaga zaakceptowania dokumentacji projektowej przez dział sieciowy.

1.11. Certyfikaty

Minimalne wymagania elementów okablowania strukturalnego to kategoria 6/ klasa E oraz RJ45 jako interfejs końcowy dla połączeń na skrętce miedzianej 4 parowej, a dla połączeń światłowodowych włókno wielodomowe 50/125mm oraz nowy standard dla sieci LAN – MT – RJ. Kategoria 6 jest najnowszym dodatkiem do standardów okablowania strukturalnego i posiada dwukrotnie szersze pasmo przenoszenia niż okablowanie Kategorii 5e. To poszerzone pasmo przenoszenia, razem ze znacznie powiększoną odpornością na zewnętrzne zakłócenia, zabezpiecza potencjał Kategorii 6, który pozwoli obsługiwać wielo-gigabitowe aplikacje. Określone w nowym standardzie specyfikacje narzucają producentom konieczność opracowania takich komponentów Kategorii 6, które będzie można dowolnie mieszać i łączyć (ang. Mix&Match) nawet z produktami konkurencji. Taka sytuacja gwarantuje użytkownikom sieci swobodę wyboru technologii lub zmianę dostawcy. Norma eliminuje również możliwość wyboru komponentów, które są tylko oznaczone symbolem "Cat.6", a w rzeczywistości nie spełniają wymagań założonych przez zatwierdzony nowy standard. Dlatego inwestor, przyszły użytkownik czy instalator okablowania powinien wiedzieć, jak odróżnić systemy RZECZYWISTEJ kategorii 6 od systemów, które tylko mają napis "Cat.6". Oprócz oznaczenia produktu istotne jest również dołączenie do niego odpowiednich certyfikatów testowania nową metodą "De-Embedded Testing" określoną dokładnie w standardzie ANSI/TIA/EIA 568-B.2 Cat.6 (załącznik E i F). Tylko komponenty, które są przetestowane tą metodą gwarantują uzyskanie RZECZYWISTEJ Kategorii 6/Klasy E. Poprzednie metody testowania nie spełniają aktualnych potrzeb i okazały się zawodne (ze względu na brak powtarzalności wyników) szczególnie przy częstotliwościach powyżej 100MHz. Dlatego by zagwarantować użytkownikowi rzeczywiste i powtarzalne parametry Kategorii 6 wymaganym jest, by na etapie składania oferty na realizację projektu wykonawca przedstawił odpowiednie certyfikaty wydane przez niezależne laboratoria uwzględniające najnowszą metodę kwalifikacji komponentów sieciowych (tj. de-embedded testing).

Wymagane są certyfikaty dla materiałów i urządzeń wykorzystanych do konstrukcji sieci LAN, WLAN. Istotne są również certyfikaty firm realizujących inwestycje, oraz to, czy pomiary są dokonywane przy użyciu certyfikowanego sprzętu pomiarowego.

Formularz nr 1

WZÓR

……
nazwa jednostki organizacyjnej

.....
Lokalny Administrator Bezpieczeństwa Informacji

Wykaz zbiorów danych osobowych w których przetwarzane są dane osobowe na Uniwersytecie Warszawskim [1]

Nazwa zbioru/bazy danych osobowych[2]	System bazy danych dla zbiorów informatycznych lub opis zbioru	Sposób zabezpieczenia i archiwizowania informacji	Zawiera także dane osób spoza UW (T/N)

[1] wykaz zbiorów dotyczy nie tylko zbiorów informatycznych również tradycyjnych np. kartoteki papierowe, teczki osobowe itp.

[2] należy dołączyć opis struktury zbiorów oraz powiązania między polami informacyjnymi w zbiorze wg podanej istrukcji.

Formularz nr 2

WZÓR

.....
nazwa jednostki organizacyjnej

.....
Lokalny Administrator Bezpieczeństwa Informacji

Wykaz budynków, pomieszczeń tworzących obszar przetwarzania danych osobowych na Uniwersytecie Warszawskim

Nazwa zbioru/bazy danych osobowych	Lokalizacja (adres)	Nr pokoju/piętro	Funkcja lokalizacji [1]	Zabezpieczenie fizyczne pomieszczenia[2]

[1] należy podać funkcję pomieszczenia: np. (A) – pokój administratorów, (U) – pokoje użytkowników zbiorów/ baz danych osobowych, (S) – serwerownia, (K) –miejsce przechowywania kopii bezpieczeństwa, archiwum itp.

[2] należy opisać system zabezpieczeń np. kraty, dodatkowe zamki, portiernia wydająca klucze uprawnionym, alarm, szyfr itp.

Formularz nr 3

WZÓR

.

.....
nazwa jednostki organizacyjnej

.....
Lokalny Administrator Bezpieczeństwa Informacji

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych

Imię i Nazwisko użytkownika	Numer wydanego upoważnienia	Okres dostępu do danych od-do	Nazwa zbioru/bazy danych osobowych

Formularz nr 4

WZÓR

UNIWERSYTET WARSZAWSKI

WNIOSEK NR [1] _____ _____

Kolejny numer /rok

O NADANIE/ UNIEWAŻNIENIE[2] UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH UNIWERSYTETU WARSZAWSKIEGO

.....

Imię i Nazwisko/ stanowisko

w.....

(nazwa jednostki organizacyjnej UW)

☐ Dane przetwarzane na nośnikach papierowych

☐ Dane przetwarzane w systemie informatycznym Identyfikator: _____

Okres obowiązywania: **NA CZAS OKREŚLONY : od ..... do .....**
NA CZAS ZGODNY Z ZATRUDN.[3]

ZAKRES UPRAWNIEŃ (DOSTĘPNYCH CZYNNOŚCI):[4]

Bazy danych/Aplikacje/ Programy umieszczone na serwerach

NAZWA	czytanie	zapis	zmiana	usunięcie

Data i podpis wnioskującego o nadanie/cofnięcie upoważnienia(Kierownika jednostki)	

Data i podpis LABI [5]	

[1] - numer nadaje lokalny ABI lub osoba prowadząca ewidencję w ramach jednostki

[2] – odpowiednie podkreślić

[3] – na czas zatrudnienia zgodny z umową o pracę w uczelni oraz zakresem obowiązków użytkownika-

[4] - należy wpisać x w odpowiednie pole (dla systemu HMS oraz USOS należy wypełnić dodatkowo Formularz zgłoszeniowy na usługę wykonywaną przez DAK, dostępny na stronie: www.it.adm.uw.edu.pl)

[5] – podpisuje lokalny administrator bezpieczeństwa informacji

Formularz nr 5

WZÓR

.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH UNIWERSYTETU WARSZAWSKIEGO

Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r.o ochronie danych osobowych, Uniwersytet Warszawski jako Administrator Danych Osobowych a w jego imieniu Administrator Bezpieczeństwa Informacji, upoważnia Panią/Pana:

.....
Imię i Nazwisko
.....
Nazwa jednostki organizacyjnej

do przetwarzania danych osobowych UW zgodnie z Wnioskiem Nr ..... oraz zobowiązuje do przetwarzania danych osobowych zgodnie z ustalonymi upoważnieniami i uprawnieniami oraz przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm. oraz wydanych na jej podstawie aktów wykonawczych.

Zobowiązuję się do nie ujawniania, w żadnej postaci i treści, informacji dotyczących danych osobowych zawartych w zbiorach Uniwersytetu Warszawskiego z wyjątkiem sytuacji, kiedy jest to niezbędne dla celów służbowych.

Przyjmuję do wiadomości, że nieprzestrzeganie powyższego obowiązku może powodować moją odpowiedzialność z tytułu ciężkiego naruszenia obowiązków pracowniczych.

Data i podpis upoważnionego	**Potwierdzam, że zostałam/em zapoznana/ny z przepisami ustawy o ochronie danych osobowych oraz stosowanymi sposobami ich zabezpieczenia**

Data i podpis LABI	

Data przyjęcia wniosku oraz podpis osoby prowadzącej ewidencję osób upoważnionych do przetwarzania danych	

Upoważnienie cofnięto dnia:

Data i podpis LABI	