Załącznik nr 1
do Zarządzenia Nr /2013
Rektora UMCS

Obowiązki osób na stanowiskach kierowniczych – bezpośrednich przełożonych służbowych osób, obsługujących oprogramowanie systemów informatycznych działających w chronionej sieci informatycznej UMCS, w zakresie zapewnienia poufności i bezpieczeństwa informacji, zawartych w bazach danych tych systemów

1. Poniższe zasady dotyczą bezpośrednich przełożonych służbowych pracowników operujących na komputerach włączonych do chronionej sieci informatycznej UMCS i obsługujących w szczególności systemy: Zintegrowany Informatyczny System Wspomagający Zarządzanie Uczelnią oparty o platformę SAP, System Dziekanatowy ALMISTOR, Uczelniany System Obsługi Studiów, Internetowa Rejestracja Kandydatów, System Elektronicznej Legitymacji Studenckiej, System Księgowy FIX, System Kadry-Płace, System Kontroli Pracowni, Strona Internetowa UMCS.
2. Naruszenie ochrony danych, zawartych w bazach danych komputerowych systemów działających w chronionej sieci informatycznej UMCS, tj. naruszenie ich poufności (nieuprawniony dostęp) oraz bezpieczeństwa (nieupoważnione niszczenie lub zmiana zapisów informacji) są przestępstwami ściganymi na podstawie art. 267-269 kodeksu karnego (Dz. U. z 1997 r. Nr 88 poz. 553 z późn. zm.); ściganiu i karze podlegają także osoby, które świadomie bądź przez zaniedbanie (także zaniedbanie nadzoru) umożliwiły innym osobom dokonanie takiego przestępstwa. W przypadku, gdy przy tego typu naruszeniu zostały ponadto ujawnione nieuprawnionym osobom trzecim dane osobowe, czyn taki jest przestępstwem ściganym na podstawie art. 49-52 ustawy o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.).
3. Każdy pracownik, który uzyskał dostęp do chronionej sieci informatycznej UMCS oraz któregoś z systemów informatycznych tj. otrzymał odpowiednie identyfikatory oraz tajne hasła, powinien być niezwłocznie przez bezpośredniego przełożonego:
    1) zaopatrzony w kopię „Instrukcji użytkowania systemów informatycznych działających w ramach chronionej sieci informatycznej UMCS" stanowiącą ***załącznik nr 2*** do niniejszego zarządzenia.
    2) wezwany do podpisania oświadczenia (wzór stanowi ***załącznik nr 3*** do niniejszego zarządzenia) o tym, iż został pouczony o obowiązku zapewnienia ochrony danych, do których ma dostęp, w zakresie ich poufności i bezpieczeństwa;
4. W przypadku gdy zakres czynności pracownika zmienił się w stopniu uzasadniającym uzyskanie nowych, dodatkowych uprawnień w zakresie dostępu do danych lub w stopniu uzasadniającym utratę części lub wszystkich uprawnień (np. pracownik dziekanatu przestał zajmować się sprawami pomocy stypendialnej a przeszedł do prowadzenia spraw toku studiów), jego przełożony jest obowiązany niezwłocznie zawiadomić administratora systemu o zaistniałej zmianie. Administrator dokona odpowiednich zmian w zakresie dostępu danego pracownika do danych.
5. W przypadku gdy pracownik, posiadający uprawnienia pozwalające na dostęp do chronionej sieci informatycznej UMCS, przestał pracować na dotychczasowym

stanowisku (przejście do innego działu, innej jednostki, rozwiązanie stosunku pracy z UMCS), jego bezpośredni przełożony jest obowiązany najpóźniej do dnia przeniesienia lub rozwiązania stosunku pracy powiadomić administratora danego systemu o zaistniałej zmianie (administrator dokona deaktywacji danego użytkownika systemu). W żadnym wypadku nie jest dopuszczalne „przekazanie" identyfikatora i hasła nowemu pracownikowi, który przyjdzie na miejsce osoby odchodzącej (celem jest uniemożliwienie osobie odchodzącej z danego stanowiska dalszego korzystania z dotychczasowych uprawnień).

6. Administrator systemu przyznaje innej osobie, która została przyjęta na miejsce osoby odchodzącej, indywidualny przypisany do tej osoby identyfikator (z hasłem startowym), dopiero po przeszkoleniu nowego pracownika i dopełnieniu formalności opisanych w ust. 3. W przypadku gdy zakres obowiązków zostaje zmieniony (rozszerzenie, ograniczenie), bezpośredni przełożony obowiązany jest zawiadomić o tym fakcie administratora systemu.
7. Dla zachowania bezpieczeństwa hasła wykorzystywane w procesie logowania są zmieniane maksymalnie co 30 dni. Bezpośredni przełożony odpowiada za nadzór nad przestrzeganiem przez pracowników powyższego obowiązku. Zastosowane są również środki systemowe mające na celu wymuszanie zmiany hasła (w przypadku takich możliwości technicznych lub organizacyjnych). Jeżeli brak jest możliwości ustawienia automatycznego wymuszania zmiany hasła o konieczności jego zmiany przypomina pracownikom komunikat zawierający niezbędne informacje o częstotliwości zmiany i złożoności hasła.
8. Procedura tworzenia konta nadawania/zmiany uprawnień w systemie SAP:
    1) użytkownik wypełnia formularz stanowiący ***załącznik nr 4*** do niniejszego zarządzenia, który następnie przesyła w wersji elektronicznej do Administratora Dziedzinowego/Kierownika Zespołu Wdrożeniowego.
    2) Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego po wprowadzeniu poziomu uprawnień (***załącznik nr 6*** do niniejszego zarządzenia), wydrukowaniu i podpisaniu przekazuje formularz w wersji papierowej administratorowi SAP.
    3) w ciągu tego samego bądź następnego dnia roboczego zostaje założone konto użytkownika SAP.
    4) użytkownik jak i Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego zostaną poinformowani o fakcie założenia użytkownika SAP poprzez e-mail.
    5) wszelkie uwagi dotyczące użytkownika SAP proszę kierować na adres: sapadm@umcs.lublin.pl.
    6) Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego jest zobowiązany do niezwłocznego poinformowania administratora systemu o konieczności zmiany uprawnień lub zaprzestania korzystania z systemu na skutek zmian organizacyjnych lub rozwiązania stosunku pracy z użytkownikiem systemu. Zmiana uprawnień jest dokonywana w oparciu o formularz stanowiący ***załącznik nr 4*** do niniejszego zarządzenia i jest rozumiana jako aktualizacja uprawnień w systemach.
9. Procedura tworzenia konta nadawania/zmiany uprawnień w innych niż SAP systemach informatycznych UMCS:
    1) użytkownik wypełnia formularz stanowiący ***załącznik nr 5*** do niniejszego zarządzenia, który następnie przesyła w wersji elektronicznej do kierownika jednostki organizacyjnej.

2) kierownik jednostki organizacyjnej po wprowadzeniu poziomu uprawnień (***załącznik nr 6*** do niniejszego zarządzenia), wydrukowaniu i podpisaniu przekazuje formularz w wersji papierowej administratorowi systemu.
3) w ciągu tego samego bądź następnego dnia roboczego zostaje założone konto użytkownika w systemie.
4) użytkownik jak i Kierownik jednostki organizacyjnej zostaną poinformowani o fakcie założenia konta użytkownika w systemie poprzez e-mail.
5) kierownik jednostki organizacyjnej jest zobowiązany do niezwłocznego poinformowania administratora systemu o konieczności zmiany uprawnień lub zaprzestania korzystania z systemu na skutek zmian organizacyjnych lub rozwiązania stosunku pracy z użytkownikiem systemu. Zmiana uprawnień jest dokonywana w oparciu o formularz stanowiący ***załącznik nr 5*** do niniejszego zarządzenia i jest rozumiana jako aktualizacja uprawnień w systemach.

10. Poziomy uprawnień w systemach informatycznych działających w chronionej sieci informatycznej UMCS określone są w ***załączniku nr 6*** do niniejszego zarządzenia.
11. Przyznane użytkownikom uprawnienia w systemach informatycznych działających w chronionej sieci informatycznej UMCS ewidencjonowane są w rejestrze, którego wzór stanowi ***załącznik nr 7*** do niniejszego zarządzenia. Dozwolone jest prowadzenie rejestru w formie elektronicznej.
12. W przypadku odejścia pracownika z UMCS, bezpośredni przełożony zobowiązany jest powiadomić o tym fakcie (najpóźniej do dnia rozwiązania stosunku pracy) służby administrujące chronioną siecią komputerową UMCS, w celu zablokowania konta sieciowego odchodzącej osoby. Analogicznego zawiadomienia należy dokonać w przypadku, gdy pracownik zmienia stanowisko pracy w obrębie UMCS. Służby administrujące systemami informatycznymi zależnie od zmiany zakresu obowiązków dokonają odpowiedniej korekty w zakresie uprawnień dostępu pracownika do poszczególnych systemów na podstawie procedur określonych w pkt 8-9.
13. Centrum Kadrowo - Płacowe jest zobowiązane do przekazywania administratorom sieci i systemów informatycznych UMCS, co najmniej raz w tygodniu, informacji dotyczących ustania stosunku pracy użytkowników systemów informatycznych działających w chronionej sieci informatycznej UMCS oraz kont poczty elektronicznej. Zakres przekazywanych danych określa ***załącznik nr 8*** do niniejszego zarządzenia. W szczególnych przypadkach Centrum Kadrowo - Płacowe realizuje powyższą procedurę niezwłocznie po otrzymaniu informacji o ustaniu stosunku pracy użytkownika sieci lub systemów informatycznych UMCS. Dopuszcza się przekazanie informacji w wersji elektronicznej na adres biuro.lubman@umcs.lublin.pl, przy czym osobami uprawnionymi do przekazywania danych w formie elektronicznej jest Dyrektor Centrum Kadrowo - Płacowego lub pisemnie przez niego upoważnieni pracownicy.

Załącznik nr 2
do Zarządzenia Nr /2013
Rektora UMCS

INSTRUKCJA
użytkowania systemów informatycznych działających w ramach chronionej sieci informatycznej UMCS – procedury ochronne

I. Informacje ogólne

1. Instrukcja dotyczy wszystkich osób mających dostęp do sieci chronionej UMCS.
2. Naruszenie ochrony danych, zawartych w bazach danych komputerowych systemów dla działających w chronionej sieci informatycznej UMCS tj. naruszenie ich poufności (nieuprawniony dostęp) oraz bezpieczeństwa (nieupoważnione niszczenie lub zmiana zapisów informacji) są przestępstwami ściganymi na podstawie art. 267-269 kodeksu karnego (Dz. U. z 1997 r. Nr 88 poz. 553 z późn. zm.); ściganiu i karze podlegają także osoby, które świadomie bądź przez zaniedbanie (także zaniedbanie nadzoru) umożliwiły innym osobom dokonanie takiego przestępstwa. W przypadku gdy przy tego typu naruszeniu zostały ponadto ujawnione nieuprawnionym osobom trzecim dane osobowe, czyn taki jest przestępstwem ściganym na podstawie art. 49-52 ustawy o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.).
3. Osoby upoważnione do dostępu do określonego zbioru informacji, zawartego w bazach danych UMCS, otrzymują do osobistego, indywidualnego użytku: jawny identyfikator (*login*) oraz tajne hasło (*password*). Z identyfikatorem użytkownika skojarzony jest zbiór informacji, do których użytkownik ma dostęp oraz przywileje pozwalające bądź jedynie na przeglądanie informacji bądź dodatkowo na dokonywanie zmian w określonym zakresie (zależnie od uprawnień-wprowadzanie nowych danych, edycja posiadanych oraz usuwanie nieaktualnych danych). Dostęp do udostępnionych użytkownikowi danych jest możliwy tylko po poprawnym podaniu identyfikatora oraz przyporządkowanego do niego hasła.
4. Niezależnie od identyfikatora i hasła, związanych z dostępem do konkretnego zbioru informacji, użytkownik może mieć przydzielone osobno: identyfikator sieciowy („konto sieciowe") i hasło uprawniające do „logowania się" w sieci chronionej UMCS (VPN). Stanowią one wstępną ochronę zasobów sieci przed osobami, które mogłyby, uzyskawszy dostęp do sieci, zakłócić jej pracę, próbować nielegalnego dostępu do danych specjalnymi środkami technicznymi lub nawet zniszczyć całe bazy danych.

II. Zasady ochrony identyfikatorów i haseł

1. Z wyżej wymienionych względów, wszyscy użytkownicy sieci chronionej UMCS, zobowiązani są do szczególnej dbałości o swoje identyfikatory i hasła, oraz są jednoosobowo odpowiedzialni za wszelkie skutki zaniedbań w tym względzie, na równi z odpowiedzialnością za umyślne działania powodujące naruszenie poufności danych lub zakłócenia w pracy tych systemów, w tym dokonywanie bezprawnych zmian w zapisach informacji, do których mają dostęp. Należy pamiętać, iż zmiana tych informacji może za sobą pociągnąć skutki finansowe i prawne.
2. Nie wolno udostępniać swojego identyfikatora sieciowego ani bazodanowego, ani tym bardziej związanych z nimi tajnych haseł innym osobom (nawet osobom bliskim i zaufanym).
3. Nie wolno udostępniać swojego identyfikatora ani hasła innym pracownikom, choćby nawet mieli identyczne uprawnienia dostępu (użyczanie swojego dostępu w sytuacji, gdy

współpracownik zapomniał swojego hasła jest niedopuszczalne). Korzystanie z identyfikatora i hasła udostępnionego przez innego pracownika jest zabronione.

4. Nie wolno – odchodząc od komputera na tyle, że przestaje się widzieć swoje stanowisko komputerowe – pozostawiać otwartej (działającej) aplikacji bazodanowej, tj. programu umożliwiającego dostęp do informacji zawartych w bazie danych systemu informatycznego. Przed opuszczeniem stanowiska pracy należy zakończyć pracę programu (w przypadku pozostawienia swobodnego dostępu do danych istnieje niebezpieczeństwo udostępnienia informacji osobom niepowołanym co jest poważnym naruszeniem zasad bezpieczeństwa ze wszystkimi tego konsekwencjami prawnymi). W celu wzmocnienia ochrony informacji wprowadza się hasłowany wygaszacz ekranu.
5. Wszelkie hasła pozwalające na dostęp do informacji należy chronić przed przypadkowym ujawnieniem osobom postronnym. W tym celu:
    1) hasła należy nauczyć się na pamięć i nigdzie go nie zapisywać;
    2) nigdy nie należy zapisywać hasła razem z identyfikatorem bądź notatką wskazującą na rolę hasła w dostępie do określonego zbioru informacji;
    3) w przypadku wystąpienia konieczności zapisania hasła (co jest w stopniu wysokim niewskazane) np. obawa zapomnienia hasła, należy zapisać hasło w sposób „zaszyfrowany”; przykładowy sposób zaszyfrowania: hasło abcd12xyz można utajnić poprzez odwrócenie znaków - zyx21dcba, bądź przestawienie grup znaków - xyz12cdab; sposób w jaki użytkownik „szyfruje” hasło powinien być łatwy do zapamiętania przez użytkownika a trudny do odgadnięcia przez inne osoby; dodatkowo zaleca się ukryć nośnik hasła w miejscu dostępnym tylko dla użytkownika;
    4) w przypadku uzasadnionej obawy, że ktoś przypadkowo lub celowo wszedł w posiadanie hasła, należy je natychmiast zmienić (w przypadku niemożności zmiany hasła należy skontaktować się z odpowiednim administratorem systemu);
    5) należy okresowo (nie rzadziej niż raz na 30 dni) dokonywać zmiany haseł dostępu.
6. W przypadku utraty hasła (jego zapomnienie) należy zwrócić się do właściwych służb informatycznych w celu uzyskania nowego hasła. Służby te nie znają i nie mogą przypomnieć utraconego hasła, mają natomiast możliwość i prawo jego zmiany na nowe.
7. Natychmiast po otrzymaniu hasła od pracownika właściwej służby informatycznej należy dokonać samodzielnie jego zmiany na hasło znane tylko użytkownikowi.
8. Ze względu na niebezpieczeństwo wprowadzenia wirusów, nie wolno na komputerach pracujących w sieci chronionej UMCS instalować ani uruchamiać jakichkolwiek innych programów, które nie zostały zakupione lub zainstalowane przez służby informatyczne. Użytkownik, który spowoduje lub umożliwi zawirusowanie komputera, spowoduje zakłócenia pracy sieci chronionej lub sprowadzi niebezpieczeństwo dla zbiorów informacji znajdujących się w posiadaniu UMCS, jest odpowiedzialny materialnie za ewentualne szkody oraz koszty prac związanych z przywróceniem prawidłowego funkcjonowania sieci chronionej.

Załącznik nr 3
do Zarządzenia Nr /2013
Rektora UMCS

.....
Nazwisko i imię

.....
Stanowisko

.....
Jednostka organizacyjna

OŚWIADCZENIE

W związku z uzyskaniem przeze mnie – wraz z odnośnymi identyfikatorami i hasłami – uprawnień dostępu do sieci chronionej UMCS oświadczam, iż uprzedzono mnie o odpowiedzialności karnej (przewidzianej w szczególności w art. 267-269 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.)) za naruszenie ochrony tych danych, a w szczególności za ich niszczenie, nieuprawnione zmienianie, wprowadzanie informacji niezgodnych z rzeczywistością, udostępnianie osobom nieupoważnionym, a także za próby dostępu do danych, do których nie mam upoważnienia. Zobowiązuję się równocześnie do przestrzegania tych przepisów oraz instrukcji o postępowaniu zapewniającym właściwą ochronę danych.

Lublin, dn. .....

.....
podpis pracownika

Załącznik nr 4
do Zarządzenia Nr /2013
Rektora UMCS

FORMULARZ REJESTRACJI UŻYTKOWNIKA/ZMIANY RÓL/BLOKADY KONTA W SYSTEMIE SAP*

***** niepotrzebne skreślić

Wypełnia użytkownik:

Nazwisko*	

*Osoba będąca właścicielem konta w SAP

Imię		**Identyfikator***	

*Wypełnić tylko w przypadku zmiany uprawnień lub blokady konta

Telefon kontaktowy	

Lokalizacja: Budynek		**Nr pokoju**	

Służbowy adres e-mail	

Wypełnia Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego:

Role do wypełnienia na odwrocie formularza*
Uwagi:

*nie dotyczy blokady konta

Proszę o założenie użytkownika SAP z rolami, które zostały określone w niniejszym dokumencie/zmianę ról/blokadę konta.*	
Podpis Administratora Dziedzinowego/Kierownika Zespołu Wdrożeniowego	

***** niepotrzebne skreślić

Przed złożeniem wypełnionego formularza należy uzyskać zgodę na założenie użytkownika SAP od osoby odpowiedzialnej za gospodarkę zasobami osobowymi jednostki.*	
Udzielam zgody na założenie użytkownika SAP UMCS/zmianę ról/blokadę konta	

*Nie dotyczy jeżeli osobą odpowiedzialną jest Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego

Wypełniony formularz należy dostarczyć do LubMAN UMCS. Konto zostaje uaktywnione w tym samym dniu lub na kolejny dzień roboczy po terminie złożenia formularza. Zarówno Użytkownik jak i kierownik jednostki organizacyjnej o założeniu konta zostaną poinformowani mailowo.

Wypełnia Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego:

Role FI

Role SD

Role ZP

Role MM

Role FIAA

Role HR

Role CO

Załącznik nr 5
do Zarządzenia Nr /2013
Rektora UMCS

FORMULARZ REJESTRACJI UŻYTKOWNIKA/ZMIANY UPRAWNIEŃ/BLOKADY KONTA W SYSTEMACH INFORMATYCZNYCH UMCS *

*niepotrzebne skreślić

Wypełnia użytkownik:

Nazwisko*	

*Osoba będąca właścicielem konta w systemie

Imię		**Identyfikator***	

*Wypełnić tylko w przypadku zmiany uprawnień lub blokady konta

Telefon kontaktowy	

Lokalizacja: Budynek		**Nr pokoju**	

Służbowy adres e-mail	

Wypełnia kierownik jednostki organizacyjnej:

Uprawnienia do wypełnienia na odwrocie formularza*
Uwagi:

*nie dotyczy blokady konta

Proszę o założenie użytkownika w systemie z uprawnieniami, które zostały określone w niniejszym dokumencie/zmianę uprawnień/blokadę konta.*	
Podpis kierownika jednostki organizacyjnej	

***** niepotrzebne skreślić

Wypełniony formularz należy dostarczyć do LubMAN UMCS. Konto zostaje uaktywnione w tym samym dniu lub na kolejny dzień roboczy po terminie złożenia formularza. Zarówno Użytkownik jak i kierownik jednostki organizacyjnej o założeniu konta zostaną poinformowani mailowo.

Wypełnia kierownik jednostki organizacyjnej:

Uprawnienia w systemie ALMISTOR/USOS*
*niepotrzebne skreślić

Uprawnienia w systemie SELS

Uprawnienia w systemie Kadry-Płace UMCS

Uprawnienia administratora/redaktora strony internetowej UMCS*
*niepotrzebne skreślić

Uprawnienia w systemie FIX

Uprawnienia w Systemie Kontroli Pracowni

Uprawnienia w Systemie Internetowej Rejestracji Kandydatów

Załącznik nr 6
do Zarządzenia Nr /2013
Rektora UMCS

POZIOMY UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH DZIAŁAJĄCYCH W CHRONIONEJ SIECI INFORMATYCZNEJ UMCS

Uprawnienia w systemie SAP

Uprawnienia w systemie ALMISTOR

Uprawnienia w systemie USOS

Uprawnienia w systemie SELS

Uprawnienia w systemie Kadry-Płace UMCS

Uprawnienia administratora strony internetowej UMCS

Uprawnienia redaktora strony internetowej UMCS

Uprawnienia w systemie FIX

Uprawnienia w Systemie Kontroli Pracowni

Uprawnienia w Systemie Internetowej Rejestracji Kandydatów

Załącznik nr 7
do Zarządzenia Nr /2013
Rektora UMCS

Rejestr przyznanych użytkownikom uprawnień w systemach informatycznych działających w chronionej sieci informatycznej UMCS

Lp.	Imię	Nazwisko	Nazwa jednostki Organizacyjnej	Data przyznania uprawnień	Data odebrania uprawnień/zmiana	Przyznane uprawnienia	Identyfikator w systemie	Uwagi

Załącznik nr 8
do Zarządzenia Nr /2013
Rektora UMCS

Wykaz użytkowników sieci i systemów informatycznych UMCS, z którymi został rozwiązany stosunek pracy

Lp.	Imię	Nazwisko	Nazwa jednostki Organizacyjnej	Data ustania stosunku pracy	PESEL	Identyfikator w systemie*	Uwagi

*opcjonalnie