ZARZĄDZENIE

Nr 74/2014

Rektora

Uniwersytetu Marii Curie-Skłodowskiej

w Lublinie

z dnia 1 grudnia 2014 r.

zmieniające Zarządzenie Nr 33/2008 Rektora UMCS z dnia 4 lipca 2008 r. w sprawie zapewnienia właściwej ochrony oprogramowania oraz danych w systemach informatycznych działających w chronionej sieci informatycznej UMCS

Na podstawie art. 66 ust. 2 ustawy z dnia 27 lipca 2005 r. – *Prawo o szkolnictwie wyższym* (tj. Dz. U. z 2012 r. Nr 572 z późn. zm.),

zarządzam:

§ 1

W Zarządzeniu Nr 33/2008 Rektora UMCS z dnia 4 lipca 2008 r. *w sprawie zapewnienia właściwej ochrony oprogramowania oraz danych w systemach informatycznych działających w chronionej sieci informatycznej UMCS,* wprowadza się następujące zmiany:

1) uchyla się dotychczasowy załącznik nr 6;
2) załączniki do powyższego zarządzenia otrzymują brzmienie określone w załącznikach nr 1, 2, 3, 4, 5, 6 i 7 do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

R E K T O R

prof. dr hab. Stanisław Michałowski

Załącznik nr 1

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, Serwis Internetowy 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 2014, poz. 1182).
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:
    a. zaopatrzony w kopię „Instrukcji użytkowania systemów informatycznych działających w ramach chronionej sieci informatycznej UMCS” stanowiącą załącznik nr 2.
    b. wezwany do podpisania oświadczenia (wzór w załączniku nr 3) 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 lub upoważniony pracownik Centrum Kadrowo-Płacowego (zgodnie z procedurami opisanymi w p. 12 i 13) 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. 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.
7. Procedura tworzenia konta, nadawania/zmiany uprawnień w systemie SAP:
    a. W celu utworzenia konta użytkownika SAP wraz z uprawnieniami do samoobsługi pracowniczej pracownik wypełnia sekcję A formularza stanowiącego załącznik nr 4. Po podpisaniu przez kierownika jednostki organizacyjnej (przełożonego pracownika) formularz zostaje przekazany administratorowi SAP.
    b. W celu zmiany uprawnień użytkownika SAP pracownik wypełnia sekcję B formularza stanowiącego załącznik nr 4 oraz przekazuje formularz do odpowiedniego Administratora Dziedzinowego/Kierownika Zespołu Wdrożeniowego, który w konsultacji z przełożonym pracownika, wprowadza wymagany poziom uprawnień w sekcji B formularza, poświadczając podpisem nadane uprawnienia. Po podpisaniu przez kierownika jednostki organizacyjnej (przełożonego pracownika) formularz zostaje przekazany administratorowi SAP.
    c. W celu zablokowania konta użytkownika SAP kierownik jednostki organizacyjnej wypełnia sekcję C formularza stanowiącego załącznik nr 4 i po podpisaniu, niezwłocznie przekazuje do administratora SAP.
    d. Administrator SAP w przypadku osobistego dostarczenia wniosku może zażądać okazania dokumentu tożsamości w celu identyfikacji wnioskodawcy. W przypadku dostarczenia

wniosku drogą korespondencyjną lub przez osoby trzecie wnioskodawca zostanie poinformowany o fakcie założenia kona użytkownika SAP poprzez służbową pocztę e-mail.

e. Założenie konta/modyfikacja uprawnień w systemie SAP może trwać do 2 dni roboczych. Konta użytkowników SAP są blokowane niezwłocznie po otrzymaniu poprawnie wypełnionego formularza.
f. Wszelkie uwagi dotyczące użytkownika SAP należy kierować na adres: sapbasis@umcs.lublin.pl.
g. Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego/Kierownik Jednostki Organizacyjnej jest zobowiązany do niezwłocznego poinformowania administratora SAP o konieczności zmiany uprawnień lub zaprzestania korzystania z systemu na skutek zmian organizacyjnych lub rozwiązania stosunku pracy z użytkownikiem systemu.

8. Procedura tworzenia konta nadawania/zmiany uprawnień:
   a. W celu utworzenia konta użytkownika wraz z nadaniem uprawnień do pracy w systemach informatycznych UMCS pracownik wypełnia sekcję A formularza stanowiącego załącznik nr 5. Po wprowadzeniu poziomu uprawnień, w konsultacji z administratorem systemu informatycznego UMCS i podpisaniu przez kierownika jednostki organizacyjnej (przełożonego pracownika) formularz zostaje przekazany administratorowi systemu informatycznego UMCS.
   b. W celu zmiany uprawnień użytkownika systemu informatycznego UMCS pracownik wypełnia sekcję A formularza stanowiącego załącznik nr 5. Po wprowadzeniu poziomu uprawnień, w konsultacji z administratorem systemu informatycznego UMCS i podpisaniu przez kierownika jednostki organizacyjnej (przełożonego pracownika) formularz zostaje przekazany administratorowi systemu informatycznego UMCS.
   c. W celu zablokowania konta użytkownika systemu informatycznego UMCS kierownik jednostki organizacyjnej wypełnia sekcję B formularza stanowiącego załącznik nr 5 i po podpisaniu, niezwłocznie przekazuje do administratora systemu informatycznego UMCS.
   d. Administrator systemu informatycznego UMCS w przypadku osobistego dostarczenia wniosku może zażądać okazania dokumentu tożsamości w celu identyfikacji wnioskodawcy. W przypadku dostarczenia wniosku drogą korespondencyjną lub przez osoby trzecie wnioskodawca zostanie poinformowany o fakcie założenia kona użytkownika systemu informatycznego UMCS poprzez służbową pocztę e-mail.
   e. Założenie konta/modyfikacja uprawnień w systemach informatycznych może trwać do 2 dni roboczych. Konta użytkowników w systemach informatycznych są blokowane niezwłocznie po otrzymaniu poprawnie wypełnionego formularza.

f. 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.

9. Przyznane użytkownikom uprawnienia w systemach informatycznych działających w chronionej sieci informatycznej UMCS ewidencjonowane są przez administratorów systemów w rejestrze, którego wzór stanowi załącznik nr 6. Dozwolone jest prowadzenie rejestru w formie elektronicznej.
10. Kierownik jednostki organizacyjnej, Administrator Dziedzinowy, Kierownik Zespołu Wdrożeniowego oraz administrator systemu jest zobowiązany co najmniej raz w roku dokonać weryfikacji przyznanych użytkownikom uprawnień w systemach informatycznych UMCS.
11. 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 punkcie 7 oraz 8.
12. 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 7. 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 a dane powinny być zabezpieczone w sposób uniemożliwiający odczytanie przez osoby nieupoważnione. Na podstawie otrzymanych informacji administratorzy sieci i systemów informatycznych UMCS niezwłocznie blokują konta użytkowników systemów informatycznych działających w chronionej sieci informatycznej UMCS.
13. Centrum Kadrowo - Płacowe jest zobowiązane do przekazywania administratorom systemów informatycznych UMCS informacji dotyczących urzędowej zmiany nazwiska, która skutkować będzie zmianą identyfikatorów, zgodnie z obowiązującymi zasadami ich tworzenia. 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 a dane powinny być zabezpieczone w sposób uniemożliwiający odczytanie przez osoby nieupoważnione.

Załącznik nr 2

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 2014 r., poz. 1182).
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:
    a. hasła należy nauczyć się na pamięć i nigdzie go nie zapisywać;
    b. nigdy nie należy zapisywać hasła razem z identyfikatorem bądź notatką wskazującą na rolę hasła w dostępie do określonego zbioru informacji;
    c. 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;

d. 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);
e. 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.
9. Użytkownik może dokonać zmiany hasła w systemie informatycznym UMCS/systemie SAP:
    a. osobiście u administratora systemu (administrator systemu może zażądać okazania dowodu tożsamości w celu identyfikacji wnioskującego),
    b. telefonicznie (administrator systemu może zadać dodatkowe pytania w celu potwierdzenia tożsamości wnioskującego),
    c. za pomocą służbowej poczty e-mail.

Załącznik nr 3

.....
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 kodeksu karnego) 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

FORMULARZ REJESTRACJI UŻYTKOWNIKA, ZMIANY RÓL, BLOKADY KONTA W SYSTEMIE SAP

Wniosek o (odpowiednie zaznaczyć):

A	Założenie konta użytkownika SAP wraz z nadaniem uprawnień do samoobsługi pracowniczej UMCS – Sekcja A
B	Nadanie/modyfikacja uprawnień użytkownika SAP – Sekcja B
C	Zablokowanie konta użytkownika SAP – Sekcja C

Sekcja A

Wypełnia pracownik:

Nazwisko*		**Imię**	

*Osoba będąca właścicielem konta w SAP

Telefon kontaktowy	

Lokalizacja: Budynek		**Nr pokoju**	

Służbowy adres e-mail	

Wnioskuję o założenie konta użytkownika SAP i nadanie uprawnień do samoobsługi pracowniczej UMCS	Data, podpis przełożonego pracownika

Sekcja B

Wypełnia pracownik:

Nazwisko	

*Osoba będąca właścicielem konta w SAP

Imię		**Identyfikator**	

Telefon kontaktowy	

Służbowy adres e-mail	

Wypełnia Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego w porozumieniu z przełożonym pracownika:

Role FI – finanse i księgowość	Podpis Administratora Dziedzinowego/Kierownika Zespołu Wdrożeniowego
Role SD – sprzedaż	

Role ZP – zamówienia publiczne	
Role MM – magazyn	
Role FIAA – ewidencja majątku	
Role HR – kadry, płace, delegacje służbowe	
Role CO – kontroling	
Role RE/PM – zarządzanie majątkiem	
Role PS – projekty/Baza Ekspertów	
Role BW – hurtownia danych	

Udzielam zgody na modyfikację ról użytkownika SAP	Data, podpis przełożonego pracownika

Sekcja C

Wypełnia przełożony pracownika:

Nazwisko	

Imię		**Identyfikator**	

Wnioskuję o zablokowanie konta użytkownika SAP	Data, podpis przełożonego pracownika

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

Załącznik nr 5

FORMULARZ REJESTRACJI UŻYTKOWNIKA, ZMIANY UPRAWNIEŃ, BLOKADY KONTA W SYSTEMACH INFORMATYCZNYCH UMCS

Wniosek o (odpowiednie zaznaczyć):

A	Założenie konta użytkownika w systemach informatycznych UMCS wraz z nadaniem uprawnień – Sekcja A
B	Nadanie/modyfikacja uprawnień użytkownika w systemach informatycznych UMCS – Sekcja A
C	Zablokowanie konta użytkownika w systemach informatycznych UMCS – Sekcja B

Sekcja A

Wypełnia pracownik:

Nazwisko	

*Osoba będąca właścicielem konta w systemie

Imię		**Identyfikator***	

*Wypełnić tylko w przypadku zmiany uprawnień

Telefon kontaktowy	

Lokalizacja: Budynek		**Nr pokoju**	

Służbowy adres e-mail	

Wypełnia przełożony pracownika w porozumieniu z administratorem systemu informatycznego:

Uprawnienia w systemie dziekanatowym ALMISTOR/USOS*
*niepotrzebne skreślić
Uprawnienia w systemie SELS/ELD
Uprawnienia w systemie Kadry-Płace UMCS (stary system kadrowo-płacowy)
Uprawnienia w systemie FIX (stary system finansowo-księgowy)

Uprawnienia w Systemie Kontroli Pracowni (SKP)
Uprawnienia w Systemie Internetowej Rejestracji Kandydatów (IRK)

Wnioskuję o nadanie/modyfikację ról użytkownika systemu informatycznego UMCS	Data, podpis przełożonego pracownika

Sekcja B

Wypełnia przełożony pracownika:

Nazwisko		**Imię**	

System Informatyczny	**Identyfikator**
ALMISTOR	
USOS	
SELS/ELD	
Kadry-Płace UMCS	
FIX	
SKP	
IRK	

Wnioskuję o zablokowanie konta użytkownika systemu informatycznego UMCS	Data, podpis przełożonego pracownika

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.

Załącznik nr 6

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 7

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

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

*opcjonalnie