Załącznik nr 1
do Zarządzenia Nr 12/2022

Obowiązki w zakresie bezpiecznego użytkowania systemów informatycznych działających w chronionej sieci informatycznej UMCS

1. Poniższe zasady dotyczą użytkowników systemów informatycznych udostępnionych w ramach działalności UMCS, zwanych dalej „Systemami Informatycznymi", działających w ramach chronionej sieci informatycznej UMCS, zwanej dalej „Siecią Chronioną" oraz ich bezpośrednich przełożonych oraz kierowników jednostek UMCS. Regulamin, w szczególności, dotyczy systemów informatycznych przetwarzających dane osobowe oraz dane wrażliwe, zgodnie z „Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE" (zwane dalej RODO) oraz krajowymi przepisami prawa powszechnego.
2. Naruszenie ochrony danych, zawartych w bazach danych komputerowych Systemów Informatycznych, tj. naruszenie ich poufności (np. nieuprawniony dostęp), integralności (np. nieuprawniona modyfikacja), dostępności (np. usunięcie danych, zakłócenie pracy systemu) oraz bezpieczeństwa (nieupoważnione niszczenie lub zmiana zapisów informacji) są przestępstwami ściganymi na podstawie art. 267-269 kodeksu karnego (Dz. U. z 2021 r. poz. 2345), 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 odrębnych przepisów prawa.
3. Każdy pracownik, który uzyskał dostęp do jakiegokolwiek Systemu Informatycznego, powinien być niezwłocznie przez bezpośredniego przełożonego:
    1) zaopatrzony w kopię „Instrukcji użytkowania Systemu Informatycznego" stanowiącą załącznik nr 2,
    2) 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 dodatkowych uprawnień lub ich odebranie, jego przełożony jest zobowiązany niezwłocznie zawiadomić administratora Systemu Informatycznego o zaistniałej zmianie. Administrator dokona odpowiednich zmian w zakresie dostępu danego pracownika do danych. Powyższa zmiana realizowana jest w oparciu o formularze stanowiące załącznik nr 4 oraz 5 do niniejszego dokumentu.

5. Niedopuszczalne jest ujawnienie swojego identyfikatora i hasła innej osobie. W szczególności nie jest dopuszczalne „przekazanie" osobistego identyfikatora i hasła nowemu pracownikowi, który przyjdzie na miejsce osoby odchodzącej (celem jest uniemożliwienie osobie odchodzącej dalszego korzystania z dotychczasowych uprawnień).
6. Hasła wykorzystywane w procesie logowania muszą być cyklicznie zmieniane. Bezpośredni przełożony odpowiada za nadzór nad przestrzeganiem przez pracowników powyższego obowiązku. Obowiązek cyklicznej zmiany hasła dotyczy również Systemów Informatycznych, w których nie ma możliwości zastosowania automatycznego wymuszania zmiany hasła.
7. Procedura tworzenia konta, nadawania/zmiany uprawnień w Systemie Informatycznym SAP:
    1) Konto użytkownika SAP zostaje utworzone w Systemie Informatycznym SAP, po podpisaniu przez pracownika umowy o pracę, a następnie wprowadzeniu jej do stosownego modułu kadrowo-płacowego systemu SAP. Nowo utworzone konto użytkownika SAP posiada podstawowe uprawnienia związane z korzystaniem przez pracownika ze standardowych funkcjonalności samoobsługi pracowniczej w zależności od przynależności do danej grupy pracowniczej.
    2) W celu nadania/zmiany uprawnień użytkownika SAP pracownik wypełnia formularz stanowiący załącznik nr 4, a następnie przekazuje go do odpowiedniego Administratora Dziedzinowego/Kierownika Zespołu Wdrożeniowego, który w konsultacji z przełożonym pracownika, wprowadza wymagany poziom uprawnień w odpowiednich polach formularza, poświadczając podpisem nadane uprawnienia. Po podpisaniu przez kierownika jednostki organizacyjnej (przełożonego pracownika) formularz zostaje przekazany administratorowi Systemu Informatycznego SAP.
    3) Konto użytkownika SAP zostaje zablokowane automatycznie, po ustaniu stosunku pracy z pracownikiem.
    4) Administrator Systemu Informatycznego SAP w przypadku osobistego dostarczenia wniosku przez pracownika 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.
    5) Modyfikacja uprawnień w Systemie Informatycznym SAP może trwać do 2 dni roboczych.
    6) Wszelkie uwagi dotyczące użytkownika SAP należy kierować na adres: sapbasis@umcs.pl.
    7) Administrator Dziedzinowy/Kierownik Zespołu Wdrożeniowego/Kierownik Jednostki Organizacyjnej jest zobowiązany do niezwłocznego poinformowania administratora Systemu Informatycznego SAP o konieczności zmiany uprawnień lub zaprzestania korzystania z Systemu Informatycznego SAP na skutek zmian organizacyjnych lub rozwiązania stosunku pracy z użytkownikiem Systemu Informatycznego SAP.

8. Procedura tworzenia konta, nadawania/zmiany uprawnień w innych niż SAP Systemach Informatycznych:
    1) Konto użytkownika w Systemie Informatycznym zostaje utworzone po wprowadzeniu umowy pracownika do systemu SAP.
    2) W celu nadania lub usunięcia uprawnień w Systemach Informatycznych przełożony pracownika wypełnia i podpisuje formularz stanowiący załącznik nr 5. Formularz należy przekazać administratorowi danego Systemu Informatycznego.
    3) W przypadku osobistego dostarczenia wniosku przez pracownika administrator Systemu Informatycznego może zażądać okazania dokumentu tożsamości w celu identyfikacji osoby.
    4) Modyfikacja uprawnień w Systemach Informatycznych następuje najpóźniej w kolejnym dniu roboczym po dniu złożenia wniosku. Konta użytkowników w Systemach Informatycznych są blokowane niezwłocznie po otrzymaniu poprawnie wypełnionego formularza.
    5) Przełożony pracownika jest zobowiązany do niezwłocznego poinformowania administratora danego Systemu Informatycznego o konieczności zmiany uprawnień lub zaprzestania korzystania z Systemu Informatycznego na skutek zmian organizacyjnych lub rozwiązania stosunku pracy z użytkownikiem Systemu Informatycznego.
9. Przyznane użytkownikom uprawnienia w Systemach Informatycznych ewidencjonowane są przez administratorów Systemów Informatycznych 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 są zobowiązani co najmniej raz w roku dokonać weryfikacji przyznanych użytkownikom uprawnień w Systemach Informatycznych.
11. W przypadku rozwiązania stosunku pracy, bezpośredni przełożony zobowiązany jest powiadomić o tym fakcie (najpóźniej do dnia rozwiązania stosunku pracy) stosowne służby administrujące Systemami Informatycznymi, w celu zablokowania konta użytkownika. 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 Informatycznych na podstawie procedur określonych w punkcie 7 oraz 8.
12. Centrum Kadrowo - Płacowe jest zobowiązane do niezwłocznego przekazywania administratorom Sieci Chronionej i Systemów Informatycznych, informacji dotyczących ustania stosunku pracy użytkowników Systemów Informatycznych. Zakres przekazywanych danych określa załącznik nr 7. Dopuszcza się przekazanie informacji w wersji elektronicznej na adres biuro.lubman@umcs.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 Chronionej i Systemów Informatycznych niezwłocznie blokują konta użytkowników Systemów Informatycznych.

13. Centrum Kadrowo - Płacowe jest zobowiązane do przekazywania administratorom Systemów Informatycznych 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.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.
14. Realizacja procedur określonych w pkt. 7 , 8, 11 oraz 12 może być oparta o dedykowane narzędzie informatyczne.

Załącznik nr 2
do Zarządzenia Nr 12/2022

INSTRUKCJA
użytkowania Systemu Informatycznego – procedury ochronne

I. Informacje ogólne

1. Instrukcja dotyczy wszystkich osób mających dostęp do Sieci Chronionej.
2. Naruszenie ochrony danych, zawartych w bazach danych komputerowych Systemów Informatycznych tj. naruszenie ich poufności (np. nieuprawniony dostęp), integralności (np. nieuprawniona modyfikacja), dostępności (np. usunięcie danych, zakłócenie pracy systemu) oraz bezpieczeństwa (nieupoważnione niszczenie lub zmiana zapisów informacji) są przestępstwami ściganymi na podstawie art. 267-269 kodeksu karnego (Dz. U. z 2021 r. poz. 2345), 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 odrębnych przepisów prawa.
3. Osoby upoważnione do dostępu do określonego zbioru informacji, zawartego w bazach danych Systemów Informatycznych, 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. Zewnętrzny dostęp do Systemów Informatycznych znajdujących się w Sieci Chronionej (spoza tej sieci) jest możliwy poprzez tzw. tunel VPN. Użytkownik może uzyskać dostęp za pomocą dodatkowej aplikacji, do której musi się zalogować udostępnionym identyfikatorem i hasłem.

II. Zasady ochrony identyfikatorów i haseł

1. Użytkownicy Sieci Chronionej, 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 Informatycznych, 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, 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 (użyczanie swojego dostępu w sytuacji, gdy współpracownik zapomniał swojego hasła jest niedopuszczalne).
4. Korzystanie z identyfikatora i hasła innego pracownika jest zabronione.
5. Przed opuszczeniem stanowiska pracy należy zakończyć działanie aplikacji udostępnionych w ramach sieci chronionej lub zablokować/wyłączyć komputer (uniemożliwić dostęp do danych osobom nieuprawnionym).
6. Identyfikatory i 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) 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,
    3) 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 administratorem Systemu Informatycznego) oraz zgłosić ten fakt Administratorowi Bezpieczeństwa Informacji,
    4) należy okresowo dokonywać zmiany haseł dostępu – o okresie ważności hasła decyduje kierownik jednostki odpowiedzialnej za zarządzanie danym Systemem Informatycznym, za pisemną zgodą Rektora UMCS.
7. W przypadku utraty hasła (jego zapomnienie) należy zwrócić się do administratora danego Systemu Informatycznego w celu uzyskania nowego hasła. Jeśli dany system pozwala na zdalne ustawienie hasła należy to zrobić samodzielnie.

8. W przypadku otrzymaniu hasła od administratora Systemu Informatycznego należy niezwłocznie dokonać jego zmiany na hasło znane tylko użytkownikowi.
9. Ze względu na niebezpieczeństwa powodowane przez złośliwe oprogramowanie zabronione jest otwieranie nieznanych załączników poczty elektronicznej, instalowanie, uruchamianie jakichkolwiek programów, które nie zostały zakupione w ramach działalności uczelni lub zainstalowane przez uprawnione służby informatyczne. Oprogramowanie to może spowodować zakłócenia pracy Sieci Chronionej i stwarza bezpośrednie zagrożenie dla bezpieczeństwa zbiorów danych informatycznych UMCS.
10. Użytkownik może dokonać zmiany hasła w Systemie Informatycznym:
    1) osobiście u administratora systemu (administrator systemu może poprosić o okazanie dokumentu tożsamości w celu identyfikacji wnioskującego),
    2) za pomocą elektronicznego formularza dostępnego pod adresem login.umcs.pl.

Załącznik nr 3

do Zarządzenia Nr 12/2022

.....

Nazwisko i imię

.....

Stanowisko

.....

Jednostka organizacyjna

OŚWIADCZENIE

W związku z uzyskaniem przeze mnie – wraz z odnośnymi identyfikatorami i hasłami – uprawnień dostępu do Sieci Chronionej 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 NADANIA/ZMIANY UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM SAP

Dane pracownika:

Imię			
Nazwisko			
Identyfikator			
Telefon kontaktowy			
Służbowy adres e-mail			
Lokalizacja: Budynek		*Nr pokoju*	

Tabela nadania/modyfikacji uprawnień:

Role w Systemie Informatycznym SAP	Nadanie uprawnień	Usunięcie uprawnień
FI – finanse i księgowość		
SD – sprzedaż		
Role MM – zamówienia publiczne		
Role MM – magazyn		
Role FIAA – ewidencja majątku		
Role HCM – kadry, płace, delegacje służbowe, pensum		
CO – kontroling		
RE/PM – zarządzanie majątkiem		
PS – projekty/Baza Ekspertów		
BASIS		

Dane przełożonego pracownika:

Imię	
Nazwisko	
Służbowy adres e-mail	
Funkcja	

Data, pieczątka i podpis przełożonego pracownika	

Wypełniony formularz należy dostarczyć do LubMAN UMCS (dopuszcza się przekazanie ww. dokumentu w postaci skanu na adres e-mail: sapbasis@umcs.pl, przy czym sam e-mail musi zostać wysłany za pomocą służbowej poczty elektronicznej 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 NADANIA, ZMIANY,USUNIĘCIA UPRAWNIEŃ W INNYCH NIŻ SAP SYSTEMACH INFORMATYCZNYCH

Dane pracownika:

Imię			
Nazwisko			
Identyfikator			
Telefon kontaktowy			
Służbowy adres e-mail			
Lokalizacja: Budynek		*Nr pokoju*	

Tabela nadania/modyfikacji uprawnień:

System Informatyczny	Nadanie uprawnień	Usunięcie uprawnień
USOS		
Microsoft 365		
SOR		
Baza Wiedzy		
VPN		
System Praktyk UMCS		
Portal PZP		
System biblioteczny		

Dane przełożonego pracownika:

Imię	
Nazwisko	
Służbowy adres e-mail	
Funkcja	

Data, pieczątka i podpis przełożonego pracownika	

Wypełniony formularz należy dostarczyć do LubMAN UMCS (dopuszcza się przekazanie ww. dokumentu w postaci skanu na adres e-mail: biuro.lubman@umcs.pl, przy czym sam e-mail musi zostać wysłany za pomocą służbowej poczty elektronicznej 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

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

Załącznik nr 7

Wykaz użytkowników Sieci Chronionej i Systemów Informatycznych, z którymi został rozwiązany stosunek pracy

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

*opcjonalnie