UNIWERSYTET MEDYCZNY W ŁODZI

Zarządzenie nr ...38... /2015
z dnia ...11 czerwca... 2015 r.
Rektora Uniwersytetu Medycznego w Łodzi

w sprawie zmiany zarządzenia nr 15/2014 z dnia 6 marca 2014 r. Rektora Uniwersytetu Medycznego w Łodzi w sprawie wprowadzenia Polityki bezpieczeństwa informacji w Uniwersytecie Medycznym w Łodzi

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, ze zm.), 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) oraz § 47 ust. 4 pkt 10 Statutu Uniwersytetu Medycznego w Łodzi z dnia 29 września 2011 r., ze zm. zarządzam, co następuje:

§ 1

W Polityce bezpieczeństwa informacji w Uniwersytecie Medycznym w Łodzi, stanowiącej załącznik nr 1 do zarządzenia nr 15/2014 z dnia 6 marca 2014 r. Rektora Uniwersytetu Medycznego w Łodzi, ze zm., wprowadza się następujące zmiany:

1) § 19 otrzymuje brzmienie:
   „§ 19. Dopuszcza się możliwość uzyskania przez pracowników Uczelni lub osoby niebędące pracownikami Uczelni zdalnego dostępu VPN do sieci informatycznej Uczelni. Zasady przyznawania dostępu VPN określa Regulamin przyznawania zdalnego dostępu VPN do sieci informatycznej Uniwersytetu Medycznego w Łodzi, stanowiący załącznik nr 13 do Polityki bezpieczeństwa.";
2) po § 25 dodaje się § 25a, który otrzymuje brzmienie:
   „§ 25a. 1. Pracownik Uczelni może uzyskać certyfikat podpisu elektronicznego umożliwiający składanie podpisów na dokumentach elektronicznych.
   2. Zasady wydawania certyfikatów podpisów elektronicznych w Uczelni określa Regulamin wydawania certyfikatów podpisów elektronicznych w Uniwersytecie Medycznym w Łodzi, stanowiący załącznik nr 24 do Polityki bezpieczeństwa.";
3) załącznik nr 13 otrzymuje brzmienie określone w załączniku nr 1 do niniejszego zarządzenia;
4) dodaje się załącznik nr 24 – Regulamin wydawania certyfikatów podpisów elektronicznych w Uniwersytecie Medycznym w Łodzi, w brzmieniu określonym w załączniku nr 2 do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR

Prof. dr hab. Paweł Górski

Otrzymują:
- jednostki organizacyjne wg rozdzielnika (zarządzenie nr 8/2014 ze zm.)
- witryna UM w Łodzi

Załącznik nr 1 do zarządzenia nr 38/2015
z dnia 11 czerwca 2015 r.
Rektora Uniwersytetu Medycznego w Łodzi

Załącznik nr 13
do Polityki bezpieczeństwa informacji
w Uniwersytecie Medycznym w Łodzi

REGULAMIN PRZYZNAWANIA ZDALNEGO DOSTĘPU VPN DO SIECI INFORMATYCZNEJ UNIWERSYTETU MEDYCZNEGO W ŁODZI

Rozdział I
Postanowienia ogólne

§ 1

1. Regulamin określa zasady przyznawania indywidualnego zdalnego dostępu VPN (*Virtual Private Network*) do sieci informatycznej Uniwersytetu Medycznego w Łodzi, zwanego dalej „Uczelnią".
2. Połączenie realizowane za pomocą zdalnego dostępu VPN, zwanego dalej „dostępem VPN", jest połączeniem szyfrowanym, umożliwiającym bezpieczne zdalne korzystanie z wybranych usług i systemów informatycznych Uczelni.

§ 2

1. Korzystanie z sieci informatycznej Uczelni za pomocą dostępu VPN powinno odbywać się na posiadających odpowiednie zabezpieczenia systemowe i kryptograficzne:
   1) komputerach PC z zainstalowanym systemem operacyjnym Microsoft: Windows Vista, Windows 7, Windows 8 lub Windows 8.1 (w wersjach 32- i 64-bitowych);
   2) urządzeniach mobilnych z zainstalowanym systemem operacyjnym iOS w wersji 7 lub nowszej.
2. Urządzenia i systemy operacyjne inne niż wymienione w ust. 1 mogą być dopuszczone do pracy zdalnej za pomocą dostępu VPN po uzyskaniu pozytywnego wyniku w testach przeprowadzonych przez Centrum Informatyczno-Telekomunikacyjne Uniwersytetu Medycznego w Łodzi, zwane dalej „Centrum IT".

Rozdział II
Przyznanie dostępu VPN

§ 3

1. Za przyznawanie dostępu VPN oraz unieważnianie certyfikatów VPN jest odpowiedzialne Centrum IT.
2. Dostęp VPN może być przyznany:
   1) pracownikom Uczelni – na wniosek kierownika jednostki organizacyjnej;
   2) osobom niebędącym pracownikami Uczelni, w związku ze świadczonymi usługami na rzecz Uczelni – na wniosek Dyrektora Centrum IT.

3. Wniosek o przyznanie dostępu VPN składany jest do Centrum IT za pośrednictwem Administratora Bezpieczeństwa Informacji, zwanego dalej „ABI". Wzór wniosku stanowi załącznik nr 1 do regulaminu.
4. Wniosek, o którym mowa w ust. 3, zawiera następujące informacje:
   1) imiona i nazwiska osób, którym ma być przyznany dostęp VPN, zwanych dalej „użytkownikami";
   2) nazwę jednostki organizacyjnej – w przypadku pracowników Uczelni;
   3) pełną nazwę i adres podmiotu zewnętrznego – w przypadku osób niebędących pracownikami Uczelni;
   4) nazwę systemu informatycznego Uczelni, do którego ma być przyznany dostęp VPN;
   5) okres, na jaki ma być przyznany dostęp VPN;
   6) datę, pieczęć imienną oraz podpis wnioskodawcy.
5. Centrum IT prowadzi ewidencję osób, które otrzymały dostęp VPN, i na żądanie udostępnia ją ABI.

§ 4

1. Dostęp VPN do systemów informatycznych przetwarzających dane osobowe może być przyznany wyłącznie użytkownikom posiadającym udzielone przez ABI aktualne upoważnienie do przetwarzania danych osobowych.
2. W przypadku przyznania dostępu VPN do systemu informatycznego nieprzetwarzającego danych osobowych użytkownik zobowiązany jest przed odbiorem certyfikatu VPN do podpisania oświadczenia o zachowaniu poufności informacji, którego wzór stanowi załącznik nr 2 do regulaminu.
3. Z obowiązku podpisania oświadczenia, o którym mowa w ust. 2, są zwolnieni użytkownicy posiadający upoważnienie do przetwarzania danych osobowych.

§ 5

1. Po otrzymaniu wniosku o przyznanie dostępu VPN, zweryfikowanego i pozytywnie rozpatrzonego przez ABI, Centrum IT generuje certyfikat VPN, a następnie za pośrednictwem poczty elektronicznej informuje użytkownika o przyznaniu dostępu VPN oraz terminie zainstalowania certyfikatu.
2. Certyfikat VPN generowany jest dla komputera lub urządzenia mobilnego wskazanego przez użytkownika.
3. Użytkownik jest zobowiązany do dostarczenia do Centrum IT komputera lub urządzenia mobilnego w celu zainstalowania certyfikatu VPN oraz dokonania konfiguracji systemu operacyjnego.
4. Przed zainstalowaniem certyfikatu VPN pracownik Centrum IT zobowiązany jest do:
   1) zweryfikowania tożsamości użytkownika;
   2) udzielenia użytkownikowi instruktażu dotyczącego korzystania z certyfikatu.
5. Użytkownik potwierdza odbiór certyfikatu VPN oraz odbycie instruktażu, o którym mowa w ust. 4 pkt 2, składając podpis na formularzu, którego wzór stanowi załącznik nr 3 do regulaminu.

Rozdział III
Zasady używania certyfikatu VPN

§ 6

1. Certyfikat VPN może być używany wyłącznie przez użytkownika, dla którego został wygenerowany.
2. Udostępnianie osobom nieuprawnionym certyfikatu VPN oraz urządzeń, na których certyfikat VPN został zainstalowany, jest zabronione.
3. W przypadku udostępniania osobie nieuprawnionej certyfikatu VPN lub urządzenia, na którym został on zainstalowany, odpowiedzialność za ewentualne szkody wyrządzone wskutek nieuprawnionego dostępu do systemów informatycznych Uczelni ponosi użytkownik certyfikatu VPN.

Rozdział IV
Unieważnienie certyfikatu VPN

§ 7

1. Centrum IT unieważnia certyfikat VPN w przypadku:
   1) utraty przez użytkownika pliku, w którym zapisano certyfikat – na wniosek użytkownika;
   2) udostępnienia certyfikatu osobom nieuprawnionym;
   3) uzasadnionego podejrzenia naruszenia wiarygodności certyfikatu.
2. Użytkownik może dokonać zgłoszenia dotyczącego unieważnienia certyfikatu za pośrednictwem służbowej poczty elektronicznej (cit@umed.lodz.pl) lub telefonicznie. Pracownik Centrum IT unieważnia certyfikat VPN niezwłocznie po otrzymaniu zgłoszenia.
3. O unieważnieniu certyfikatu VPN pracownik Centrum IT niezwłocznie informuje użytkownika.
4. Niezależnie od przyczyny unieważnienia certyfikatu VPN, pracownik Centrum IT wypełnia i podpisuje formularz, którego wzór stanowi załącznik nr 3 do niniejszego regulaminu. Podpisanie formularza jest równoznaczne z zakończeniem procedury unieważniania certyfikatu VPN.
5. Po unieważnieniu certyfikatu VPN użytkownik może ubiegać się o ponowne przyznanie dostępu VPN zgodnie z przepisami § 3-5.

Rozdział V
Postanowienia końcowe

§ 8

W przypadku naruszenia przepisów niniejszego regulaminu mają zastosowania przepisy ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (t.j. Dz. U. z 2014 r. poz. 1502, ze zm.) oraz przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2014 poz. 121, ze zm.).

Załącznik nr 1
do Regulaminu przyznawania zdalnego dostępu VPN
do sieci informatycznej Uniwersytetu Medycznego w Łodzi

WNIOSEK O PRZYZNANIE ZDALNEGO DOSTĘPU VPN DO SIECI INFORMATYCZNEJ UNIWERSYTETU MEDYCZNEGO W ŁODZI

Lp.	Imię i nazwisko użytkownika	Nazwa jednostki organizacyjnej/nazwa i adres podmiotu zewnętrznego*	Okres, na który ma być przyznany dostęp VPN	Nazwa systemu informatycznego, do którego ma być przyznany dostęp VPN
1.				
2.				
3.				
4.				
5.				

.....
(data, pieczęć imienna i podpis Administratora Bezpieczeństwa Informacji)

.....
*(data, pieczęć imienna i podpis kierownika jednostki organizacyjnej /dyrektora Centrum Informatyczno-Telekomunikacyjnego)**

* W przypadku osób niebędących pracownikami Uniwersytetu Medycznego w Łodzi.

Załącznik nr 2
do Regulaminu przyznawania zdalnego dostępu VPN
do sieci informatycznej Uniwersytetu Medycznego w Łodzi

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI INFORMACJI

Ja, niżej podpisana/y.....
(imię i nazwisko)

zatrudniony w .....
(nazwa jednostki organizacyjnej Uczelni/nazwa i adres podmiotu zewnętrznego)*

zobowiązuję się zachować w tajemnicy informacje uzyskane za pomocą zdalnego dostępu VPN do następujących systemów informatycznych Uniwersytetu Medycznego w Łodzi: .....

.....

.....
(data i czytelny podpis osoby składającej oświadczenie)

* W przypadku osób niebędących pracownikami Uniwersytetu Medycznego w Łodzi.

Załącznik nr 3
do Regulaminu przyznawania zdalnego dostępu VPN
do sieci informatycznej Uniwersytetu Medycznego w Łodzi

POTWIERDZENIE ODBIORU/UNIEWAŻNIENIA* CERTYFIKATU VPN

Dla: .....
(imię i nazwisko użytkownika)

.....
*(nazwa jednostki organizacyjnej Uczelni/nazwa i adres podmiotu zewnętrznego**)*

DANE CERTYFIKATU VPN

Lp.	Numer seryjny certyfikatu VPN/CN	Data odbioru certyfikatu VPN	Podpis użytkownika potwierdzającego odbiór certyfikatu VPN oraz udzielenie instruktażu	Data ważności certyfikatu VPN	Data unieważnienia certyfikatu VPN	Podpis pracownika Centrum IT potwierdzającego unieważnienie certyfikatu VPN
1.						
2.						
3.						
4.						
5.						

* Niewłaściwe skreślić.
** W przypadku osób niebędących pracownikami Uniwersytetu Medycznego w Łodzi.

Załącznik nr 2 do zarządzenia nr 38./2015
z dnia ....11. czerwca..... 2015 r.
Rektora Uniwersytetu Medycznego w Łodzi

Załącznik nr 24
do Polityki bezpieczeństwa informacji
w Uniwersytecie Medycznym w Łodzi

REGULAMIN WYDAWANIA CERTYFIKATÓW PODPISÓW ELEKTRONICZNYCH W UNIWERSYTECIE MEDYCZNYM W ŁODZI

Rozdział I
Postanowienia ogólne

§ 1

1. Regulamin określa procedury wydawania certyfikatów podpisów elektronicznych w Uniwersytecie Medycznym w Łodzi, zwanym dalej „Uczelnią".
2. Za wydawanie i unieważnianie certyfikatów podpisów elektronicznych jest odpowiedzialne Centrum Informatyczno-Telekomunikacyjne Uniwersytetu Medycznego w Łodzi, zwane dalej „Centrum IT".

§ 2

1. Przez certyfikat podpisu elektronicznego wydawanego przez Centrum IT rozumie się elektroniczne zaświadczenie przyporządkowujące dane służące do weryfikacji podpisu elektronicznego do osoby składającej podpis elektroniczny oraz umożliwiające identyfikację tej osoby.
2. Podpis elektroniczny stosowany w Uczelni oparty jest na usłudze katalogowej *Active Directory* (hierarchicznej bazie danych). Umożliwia weryfikację tożsamości autora dokumentu, datę sygnowania dokumentu oraz zapewnia zachowanie niezmienności dokumentu od momentu złożenia podpisu.
3. Do zapewnienia prawidłowego korzystania z podpisów elektronicznych wymagany jest system operacyjny Microsoft: Windows Vista, Windows 7, Windows 8 lub Windows 8.1 (w wersji *professional* lub nowszej).
4. Systemy operacyjne inne niż wymienione w ust. 3 mogą być dopuszczone do stosowania po uzyskaniu pozytywnego wyniku w testach przeprowadzonych przez Centrum IT.

Rozdział II
Wydanie certyfikatu podpisu elektronicznego

§ 3

1. Osobą uprawnioną do uzyskania certyfikatu podpisu elektronicznego jest wyłącznie pracownik Uczelni.
2. Wydanie certyfikatu podpisu elektronicznego następuje na wniosek pracownika Uczelni, zwanego dalej „wnioskodawcą" lub „użytkownikiem", po uzyskaniu pisemnej zgody

kierownika jednostki organizacyjnej oraz Administratora Bezpieczeństwa Informacji. Wzór wniosku stanowi załącznik nr 1 do niniejszego regulaminu.

3. Wniosek, o którym mowa w ust. 2, wnioskodawca składa osobiście w Centrum IT.
4. Certyfikat podpisu elektronicznego wydawany jest na czas określony.

§ 4

1. Uzyskanie certyfikatu podpisu elektronicznego jest możliwe wyłącznie w przypadku posiadania aktywnego imiennego konta domenowego w usłudze katalogowej *Active Directory*.
2. Wnioskodawca przy pomocy pracownika Centrum IT:
   1) wysyła ze swojego konta domenowego żądanie wygenerowania certyfikatu;
   2) ustala kody (PIN/PIN SO/PUK) zabezpieczające dostęp do karty kryptograficznej, które wprowadza się do czytnika karty kryptograficznej.
3. Centrum IT generuje certyfikat podpisu elektronicznego, a następnie zapisuje go na karcie kryptograficznej.
4. Karta kryptograficzna z zapisanym certyfikatem podpisu elektronicznego oraz czytnik karty kryptograficznej z zapisanymi kodami przekazywane są użytkownikowi, który potwierdza ich odbiór oraz udzielenie instruktażu przez pracownika Centrum IT, składając podpis na formularzu, którego wzór stanowi załącznik nr 1 do niniejszego regulaminu.
5. Przed wydaniem karty kryptograficznej oraz czytnika karty pracownik Centrum IT zobowiązany jest do:
   1) zweryfikowania tożsamości użytkownika certyfikatu;
   2) udzielenia użytkownikowi instruktażu dotyczącego korzystania z certyfikatu.
6. Dla zapewnienia prawidłowego funkcjonowania karty kryptograficznej oraz czytnika Centrum IT instaluje na komputerze użytkownika odpowiednie oprogramowanie.

Rozdział III
Zasady używania certyfikatu podpisu elektronicznego

§ 5

1. Certyfikat podpisu elektronicznego wydany przez Centrum IT nie jest kwalifikowanym certyfikatem w rozumieniu przepisów ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (t.j. Dz. U. z 2013 r. poz. 262, ze zm.). Podpis elektroniczny weryfikowany za pomocą tego certyfikatu nie wywołuje skutków prawnych określonych w ustawie o podpisie elektronicznym i nie może być używany do podpisywania dokumentów elektronicznych wysyłanych przez jednostki organizacyjne Uczelni do podmiotów zewnętrznych.
2. Podpis elektroniczny weryfikowany za pomocą certyfikatu wydanego przez Centrum IT służy wyłącznie do podpisywania dokumentów elektronicznych przesyłanych w wewnętrznym obiegu dokumentów Uczelni, a dokumenty elektroniczne nim opatrzone są traktowane jako równoważne dokumentom opatrzonym podpisem własnoręcznym.

§ 6

1. Certyfikat podpisu elektronicznego może być używany wyłącznie przez użytkownika, dla którego został wygenerowany.
2. Złożenia podpisu elektronicznego dokonuje się za pomocą przeznaczonego do tego celu czytnika karty kryptograficznej, podłączonego do portu USB komputera lub urządzenia

mobilnego, oraz współpracującego z nim oprogramowania kryptograficznego zainstalowanego na karcie kryptograficznej, chroniącego certyfikat podpisu elektronicznego.

3. Złożenie podpisu elektronicznego jest możliwe wyłącznie po podaniu zabezpieczającego kodu PIN.
4. Zabrania się udostępniania osobom nieuprawnionym certyfikatu podpisu elektronicznego, karty kryptograficznej, czytnika karty kryptograficznej oraz haseł i kodów (PIN/PIN SO/PUK) do karty kryptograficznej.
5. W przypadku wygaśnięcia lub unieważnienia certyfikatu podpisu elektronicznego, lub ustania stosunku pracy, użytkownik jest zobowiązany do niezwłocznego zwrotu do Centrum IT karty kryptograficznej oraz czytnika karty.

Rozdział IV
Unieważnienie certyfikatu podpisu elektronicznego

§ 7

1. Centrum IT unieważnia certyfikat podpisu elektronicznego w przypadku utraty przez użytkownika pliku, w którym zapisano certyfikat – na wniosek użytkownika, lub w przypadku udostępnienia certyfikatu osobom nieuprawnionym.
2. Użytkownik może dokonać zgłoszenia dotyczącego unieważnienia certyfikatu podpisu elektronicznego za pośrednictwem służbowej poczty elektronicznej (cit@umed.lodz.pl) lub telefonicznie. Pracownik Centrum IT unieważnia certyfikat podpisu elektronicznego niezwłocznie po otrzymaniu zgłoszenia.
3. O unieważnieniu certyfikatu podpisu elektronicznego pracownik Centrum IT niezwłocznie informuje użytkownika.
4. Niezależnie od przyczyny unieważnienia certyfikatu podpisu elektronicznego, pracownik Centrum IT wypełnia i podpisuje formularz, którego wzór stanowi załącznik nr 1 do niniejszego regulaminu. Podpisanie formularza jest równoznaczne z zakończeniem procedury unieważniania certyfikatu podpisu elektronicznego.
5. Po unieważnieniu certyfikatu podpisu elektronicznego użytkownik może ubiegać się o jego ponowne wydanie zgodnie z przepisami § 3 i 4.

WNIOSEK O WYDANIE CERTYFIKATU PODPISU ELEKTRONICZNEGO

DANE WNIOSKODAWCY:

Imię i nazwisko:	
Nazwa jednostki organizacyjnej:	

.....
(data, pieczęć imienna i podpis kierownika jednostki organizacyjnej)

.....
(data i czytelny podpis wnioskodawcy)

.....
(data, pieczęć imienna i podpis Administratora Bezpieczeństwa Informacji)

DANE CERTYFIKATU PODPISU ELEKTRONICZNEGO:
(wypełnia pracownik Centrum Informatyczno-Telekomunikacyjnego)

Identyfikator żądania:	
Numer seryjny certyfikatu:	
Okres ważności certyfikatu:	
Data wygaśnięcia certyfikatu:	
Numer karty kryptograficznej:	
Numer seryjny czytnika:	

Potwierdzam odbiór karty kryptograficznej wraz z zainstalowanym certyfikatem podpisu elektronicznego i czytnikiem karty oraz przeprowadzenie instruktażu przez pracownika Centrum Informatyczno-Telekomunikacyjnego w zakresie ich obsługi.

.....
(data i czytelny podpis wnioskodawcy)

Data unieważnienia certyfikatu podpisu elektronicznego/Data zwrotu karty kryptograficznej i czytnika karty*:

.....
(data, pieczęć imienna i podpis pracownika Centrum Informatyczno-Telekomunikacyjnego)

* Niepotrzebne skreślić.