



РЕПУБЛИКА СРБИЈА
ИНСТИТУТ ЗА НЕОНАТОЛОГИЈУ
Бр. 2780/2
16 JUL 2024 год.
БЕОГРАД, Краља Милутина број 50

ИНСТИТУТ ЗА НЕОНАТОЛОГИЈУ

ПРАВИЛНИК

О БЕЗБЕДНОСТИ ИНФОРМАЦИОНОГ СИСТЕМА

Мршић Сања

ПРАВИЛНИК САЧИНИЛА:

Сања Мршић, дипл.инж. електротехнике

Руководилац послова информационих система и технологија

Јул, 2024. године

На основу чл. 8. Закона о информационој безбедности ("Сл. гласник РС", бр. 6/2016, 94/2017 и 77/2019) и чл. 24. Статута Института за неонатологију, Управни одбор Института доноси

ПРАВИЛНИК

О БЕЗБЕДНОСТИ ИНФОРМАЦИОНОГ СИСТЕМА ИНСТИТУТА ЗА НЕОНАТОЛОГИЈУ

Члан 1.

Овим правилником уређују се функционисање, развој и начин коришћења ресурса информационог система Института за неонатологију у Београду (у даљем тексту: информациони систем), као и мере његовог обезбеђивања и заштите. Правилник се примењује на све запослене у Институту за неонатологију, као и на све привремене кориснике информационог система.

Члан 2.

Поједини изрази употребљени у овом Правилнику имају следеће значење:

- Информациони систем чине: рачунарска и комуникациона опрема (рачунари, штампачи, мрежни уређаји, уређаји за непрекидно напајање електричном енергијом, каблови...), рачунарски програми и подаци неопходни за исправан рад информационог система;
- Системска администрација је скуп послова којима се одржава функционалност информационог система;
- Администратори информационог система су запослени у одговарајућој организационој јединици Института за неонатологију (надлежна служба: Техничка служба), који одржавају послове системске администрације информационог система;
- Корисници информационог система су сви запослени у Институту за неонатологију или друга лица којима су дата стална или привремена права за коришћење информационог система од стране овлашћене особе (директора), при чему је у том случају обавезно пријављивање корисничким именом;

- Корисничко име и лозинка су подаци који служе за приступ информационом систему;
- Системски програми су скуп програма који управљају радом рачунара (оперативни систем, базе података, антивирусни програм и сл.);
- Апликативни програми су програми које корисници извршавају на рачунару (програми за куцање текста, израду табела, рад са базама података, обраду слика и слично);
- IP адреса представља привремену или сталну идентификацију сервера и/или радне станице у оквиру рачунарске мреже;
- Домен је назив који идентификује јединствену радну групу коју чине сви рачунари, штампачи, радне јединице и корисници у оквиру мреже;
- Доменска полиса је назив за правило којим се директно одређују права и наследна својства свих чиниоца домена;
- Сервер је централни рачунар у мрежи који контролише домен. На серверу су одређене доменске полисе, и на њему се врши централно складиштење података које садржи целокупну базу свих корисника и програма који су њима придружени. Уколико постоји више сервера у систему, они врше следеће послове: DC (domain controller, контролише рад рачунара и корисника), WEB сервер (контролише везу са Интернетом), MAIL сервер (размена електронских порука), APPLICATION сервер (апликативни сервер - на њему се налазе инсталирани програми - апликације), DATABASE сервер (на њему су базе података), итд;
- Радна станица је рачунар на коме запослени обављају своје послове.
- Потрошни материјал обухвата магнетне и оптичке медијуме за складиштење података (CD и DVD медијуме), тонере за штампаче и други материјал.
- VPN (Virtual Private network — Виртуелна приватна мрежа) — мрежни сервис који омогућава приступ комплетној мрежној инфраструктури са удаљене локације.
- NAS (Network-attached storage — Мрежни систем складишта) — централизовани систем складиштења података на мрежни уређај у коме се налази складишни медијуми.

I РАЧУНАРИ, РАЧУНАРСКА И ПЕРИФЕРНА ОПРЕМА

Члан 3.

Рачунари који се налазе у организационим јединицама Института за неонатологију су власништво Института за неонатологију, осим ако то није другачије документовано.

Члан 4.

Рачунар се може користити само за обављање послова из надлежности Института за неонатологију. Коришћење рачунара за личне потребе није дозвољено, није дозвољено обављање послова изван пословне природе, нити корисник има право да приватне податке чува и складиши на пословним рачунарима.

Свим запосленима је омогућен несметани рад на рачунарима Института за неонатологију. Приступ рачунарима за рад запосленог у Институту је неометано омогућен, осим у случају злоупотребе информационог система, при чему се раднику доставља решење о привременој/трајној забрани коришћења информационог система од стране директора Института.

Запосленима се забрањује самоиницијативно постављање корисничких шифара на рачунар који користе више запослених, и било која акција која ограничава коришћење рачунара у Институту за неонатологију, а који је предвиђен за рад у здравственом информационом систему.

II ИДЕНТИФИКАЦИЈА КОРИСНИКА ИНФОРМАЦИОНОГ СИСТЕМА

Члан 5.

Информациони систем се може користити само за обављање послова из надлежности Института за неонатологију.

За планирање развоја информационог система, системску администрацију и одржавање задужена је Техничка служба, која обавља послове по налогу директора Института за неонатологију.

Само администратори информационог система могу имати администраторске привилегије у информационом систему.

Администратори информационог система могу бити искључиво запослени у Техничкој служби Института за неонатологију, као и друга лица које именује директор Института за неонатологију.

Члан 6.

Сваки корисник се идентификује својим корисничким именом и својом лозинком и дужан је да се одјави када заврши посао, при чему је корисничко име јавни податак, а лозинка тајни податак.

Корисник је дужан да чува своју лозинку, не одаје је другим лицима и сноси одговорност уколико буде злоупотребљена.

Корисничко име одређује администратор информационог система и састоји се од имена и презимена корисника. Уколико постоји више корисника који би имали исто корисничко име, разлику одређује администратор система у договору са корисником коме креира корисничко име.

Нови корисник у Институту у зависности од радног места треба да добије кориснички налог за коришћење информационог система. Почетну корисничку лозинку поставља администратор система и подразумева само име запосленог.

Корисник је дужан да промени иницијалну лозинку. Сваки корисник је обавезан да памти своју лозинку и да је мења у складу са потребама. Лозинка би требало да има најмање 6 карактера од којих најмање два треба да су бројеви и да не буду повезана са корисником (по правилу не би требало користити имена чланова породице, датуме и сл.).

Запосленом који из било ког разлога више не ради на Институту администратор информационог система укида кориснички налог по налогу начелника/шефа службе.

Класификациони електронски сертификат (токен) се добија на име корисника/запосленог за потребе послова Института, и у ту сврху се искључиво користи. Рок важења му је 3 или 5 година, и не може се мењати услед механичких оштећења.

За податке унете у систем са одређеног корисничког налога због потребе посла одговоран је корисник коме припада тај кориснички налог, и за исте одговара кривично и материјално.

Члан 7.

Администратор информационог система је овлашћен од стране директора Института да може опоменути корисника информационог система који се не придржава овог Правилника и тиме угрожава безбедност информационог система.

Администратор информационог система такође може привремено ускратити приступ кориснику који угрожава безбедност информационог система. Уколико корисник након опомене и привременог ускраћивања приступа информационом систему понови радње којима угрожава безбедност информационог система, администратор информационог система може, уз сагласност директора Института за неонатологију, трајно ускратити приступ том кориснику.

III РАЧУНАРСКИ ПРОГРАМИ

Члан 8.

На основу потребе запосленог за коришћење рачунара, Техничка служба Института за неонатологију је дужна да одреди системске и апликативне програме који ће се користити на појединим рачунарима.

Системске и апликативне програме инсталирају администратори информационог система. Строго је забрањена свака самоиницијативна набавка и инсталација системских и апликативних програма без консултације са администраторима.

Кориснику рачунара је забрањено инсталирање апликативног софтвера (програма, игара), као и снимање неовлашћеног садржаја (музика, филмови). У случају непоштовања наведеног и настајања даљих проблема услед непридржавања поменутих забрана, администратори су дужни да одмах предузму активности које ће довести до уклањања уочених слабости рачунара због злоупотребе система.

Члан 9.

Уколико постоји потреба за инсталацијом додатних апликативних програма у оквиру Института за неонатологију, захтев се упућује администраторима у писменој/усменој форми.

У случају да је потребно да се изврши инсталација апликативних програма других лица ван Института за неонатологију, потребно је поднети захтев у писменој/усменој форми администраторима.

IV РАЗМЕНА ПОДАТАКА, ИНТЕРНЕТ И ЕЛЕКТРОНСКА ПОШТА

Члан 10.

Приступ интернету обезбеђују администратори информационог система Института.

Сви корисници, пошто користе интернет на рачунарима, морају се придржавати мера заштита од вируса. Приликом коришћења интернета треба избегавати сумљиве WEB странице, обзиром да то може проузроковати проблеме – неприметно инсталирање шпијунских програма и слично. Сваки рачунар је адекватно подешен, и инсталiran му је антивирусни програм.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави администраторима.

Члан 11.

Свако ко користи интернет и електронску пошту треба да поступа по међународним конвенцијама и правилима понашања.

Корисницима који су прикључени на информациони систем је забрањено самостално прикључење на интернет (прикључење преко сопственог модема или преко било којег мрежног медијума), при чему администратор информационог система може укинути приступ интернету у случају доказане злоупотребе истог.

Рачунар на коме је корисник самостално инсталирао 5G модем — преносиви кућни интернет мреже (A1, Yettel или MTS), биће искључен из техничке подршке и биће сачињена белешка коју администратор информационог система прослеђује начелнику/шефу службе.

Корисници информационог система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у информациони систем. Сваки рачунар чији се корисник прикључује на интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врше администратори.

Строго је забрањено гледање филмова и спорских садржаја, и играње игрица на рачунарима и "крстарење" ВЕБ страницама које садрже порнографски и остали недоличан садржај, као и самовољно преузимање истих са интернета.

Строго је забрањено коришћење друштвених мрежа (Facebook, Instagram, Twitter) које представљају најпопуларнији облик комуникације. Такође, строго је забрањено и фотографисање пацијената и постављање фотографија и сличних видео записа на друштвене мреже.

На серверима и радним станицама се смеју чувати само подаци стриктно неопходни за послове и не смеју се снимати слике, музика, филмови и игрице, који ће у том случају бити обрисани са радне станице.

Уколико постоји потреба за преузимањем одређених садржаја са интернета, при чему ти садржаји нису у директној вези са описом послова тог радног места, захтев треба упутити администраторима у писменој форми, који су дужни да процене оправданост захтева у року од 72 часа.

IV УДАЉЕН ПРИСТУП ИНФОРМАЦИОНОМ СИСТЕМУ

Члан 12.

Инфраструктури Институту за неонатологију је могуће приступити са удаљене локације путем VPN конекције. Сложени приступ је омогућен без посебног одобрења директора Института за неонатологију. Под радом на даљину подразумева се: рад ван просторија Института, рад од куће и виртуално радно окружење.

Члан 13.

Рад на даљину је омогућен за све запослене у Институту за неонатологију уколико надређени из службе захтева (додатни) рад од куће због потребе посла. Администратори намештају приступ на рачунар у Институту који ће се користити са удаљене локације.

V ЗАШТИТА ИНФОРМАЦИОНОГ СИСТЕМА

Члан 14.

Заштита информационог система подразумева безбедност података од брисања, неовлашћеног приступа, заштиту од неовлашћене измене, заштиту од вируса и свих других видова угрожавања података.

Правилним коришћењем информационог система од стране корисника, односно коришћењем у складу са одредбама овог Правилника, сваки податак односно документ ће бити заштићен.

Администратори информационог система су одговорна лица за комплетну заштиту информационог система.

Члан 15.

Забрањено је вршење увида у електронску евиденцију пацијената, и то у здравствене и опште податке пацијената, уколико то није у склопу вршења лекарске дужности и дужности медицинске сестре за конкретног пацијента.

Администратори у сваком тренутку имају увид у то ко од запослених и у које време је отварао и прегледао електронски досије пацијената. Сваки улазак у досије пацијента се региструје, иако је запослени само гледао податке без икаквих уноса и вршења промена.

Кршење одредби овог члана представља повреду радне обавезе, односно непоштовање радне дисциплине у складу са Законом о раду.

Члан 16.

Сваки документ који је од значаја треба чувати на серверу или медијуму. Ако се на овај начин врши архивирање (чување) података, подаци су безбедни од неовлашћеног коришћења и случајног брисања.

Спомни медијум (ЦД и ДВД, као и екстерни хард диск или УСБ флеш) је нопуздан за трајно коришћење и требало би га користити само за пренос података.

Члан 17.

Политиком безбедности информационог система нарочито се уређују принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности овог система, као и овлашћења и одговорности у вези са овом безбедношћу и ресурсима тог система. Институт за неонатологију је дужан да политику безбедности информационог система усклађује са променама у окружењу и у самом информационом систему.

Члан 18.

Ради превентивног одржавања информационог система у одређеним временским размацима врши се замена рачунарске и комуникационе опреме и делова којима је истекао рок трајања, или код кога је настао квар.

Послове из овог Правилника обављају администратори Института за неонатологију.

Члан 19.

За успешну заштиту од вируса, администратор информационог система треба на сваком рачунару да инсталира антивирус програм и да редовно врши допуну антивирусних дефиниција. Забрањен је сваки покушај корисника да неутралише заштиту од вируса. Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносивих медија.

VI КАЗНЕНЕ ОДРЕДБЕ

Члан 20.

Запослени у Институту за неонатологију чини повреду радне обавезе уколико:

- уступи корисничко име и лозинку другој особи;
- користи корисничко име и лозинку друге особе;
- улази у електронски здравствени картон пацијента, изузев по службеној дужности;
- у непосредној близини рачунара конзумира храну, кафу и пиће;
- прикључи велике кориснике струје (на пример: решо, грејалица, клима уређај) на фазу где је прикључен рачунар;
- прикључи на уређај за непрекидно напајање електричном енергијом штампач или било који други потрошач електричне енергије;
- не извршава редовно ажурирање садржаја сајта Института за неонатологију (важи за администраторе информационог система);
- покуша да изврши самоиницијативну инсталацију било ког рачуарског програма или копира инсталiranе програме без сагласности администратора;
- покуша и/или уради прикључење било ког хардверског уређаја (рачунара, штампача и сл.) на информациони систем Института за неонатологију без знања администратора;
- на било који начин уноси или износи податке (путем интернета, имејла, помоћу преносивих медијума - дискете, ЦД и ДВД и сл.) без сагласности и провере од стране свог непосредног руководиоца што се тиче садржине, и без консултација са администраторима, а у вези са подацима из здравственог информационог система;
- корисник након опомене и привременог ускраћивања приступа Информационог систему понови радње којима угрожавају безбедност информационог система;
- ограничи коришћење ресурса информационог система другим запосленима у Институту за неонатологију;
- "крстари" ВЕБ страницама које садрже порнографски и остали недоличан садржај, као и ако самоиницијативно преузима исте са интернета;
- самоиницијативно запослени узме рачунар/лаптоп из Института и однесе на коришћење кући, без знања администратора и свог надређеног;
- користи друштвене мреже (Facebook, Instagram, Twitter) на рачунару.

VII ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 21.

Измене и допуне овог Правилника врши се на начин и по поступку за његово доношење.

Члан 22.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли Института, а примењује се по добијању свих сагласности.

УПРАВНИ ОДБОР ИНСТИТУТА ЗА НЕОНАТОЛОГИЈУ
ЗАМЕНИК ПРЕДСЕДНИКА УПРАВНОГ ОДБОРА



Др Славица Миљеновић, спец. педијатрије

Овај Правилник објављен је на огласној табли Института дана 17.07.2024. године, што потврђује:

ПОМОЋНИК ДИРЕКТОРА ЗА ПРАВНЕ, ТЕХНИЧКЕ И ДРУГЕ ПОСЛОВЕ



Весна Новаковић, дипл. правник