Дома Здравља „Стари град“
Београд

Објављено на огласној табли:_____
Скинуто са огласне табле: _____

Број: УО-120/6
Датум: 19.10.2021.

На основу члана 8. Закона о информационој безбедности ("Службени гласник РС", бр. 6/2016, 94/2017 и 77/2019) и члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја ("Службени гласник РС", број 94/2016 године), члана 119. став 1. тачка 2) Закона о здравственој заштити ("Сл. гласник РС", бр. 25/2019) и члана 37. став 1. тачка 2) Статута Дома здравља “Стари град“ број 465 од 10.02.2021. године, Управни одбор на седници одржаној дана 19.10.2021. године донео је:

ПРАВИЛНИК
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНИХ СИСТЕМА ДОМА ЗДРАВЉА „СТАРИ ГРАД“ БЕОГРАД

Предмет
Члан 1.

Овим Правилником се ближе дефинишу мере заштите информационо-комуникационих система Дома Здравља „Стари Град“ Београд (у даљем тексту: Дома Здравља), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса у Дому Здравља.

Циљеви
Члан 2.

Циљеви доношења овог Правилника су:

1) допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
2) минимизација безбедносних инцидената;
3) допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистентне контроле свих компонената информационо - комуникационог система (у даљем тексту: ИКТ систем).

Обавезност
Члан 3.

Овај Правилник је обавезујући за све унутрашње организационе јединице Дома Здравља и за све кориснике информатичких ресурса, као и за сва трећа лица која користе информатичке ресурсе Дома Здравља.

Непоштовање овог Правилника повлачи дисциплинску одговорност корисника информатичких ресурса.

За праћење примене овог Правилника надлежан је Руководилац послова информационих система и технологије.

Појмови
Члан 4.

Поједини изрази употребљени у овом Правилнику имају следеће значење:

1) *ИКТ систем* је технолошко-организациона целина која обухвата:
- електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
- уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
- податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКТ системом;
- све типове системског и апликативног софтвера и софтверске развојне алате.

2) *информациона безбедност* представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

3) *тајност* је својство које значи да податак није доступан неовлашћеним лицима;

4) *интегритет* значи очуваност изворног садржаја и комплетности податка;

5) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) *аутентичност* је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

7) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

8) *управљање ризиком* је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

9) *инцидент* је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система;

Мере заштите
Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Дома Здравља, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Информатички ресурси Дома здравља
Члан 6.

Информатички ресурси Дома Здравља су сви ресурси који садрже пословне информације Дома Здравља у електронском облику или служе за приступ корисника ИКТ систему укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и слично.

Предмет заштите
Члан 7.

Предмет заштите обухвата:

1) хардверске и софтверске компоненте информатичких ресурса;
2) податке који се обрађују или чувају на информатичким ресурсима;
3) корисничке налоге и друге податке о корисницима информатичких ресурса Дома Здравља.

Корисник информатичких ресурса
Члан 8.

Корисник информатичких ресурса јесте постављено лице, запослено лице на неодређено или одређено време, лице ангажовано по основу уговора, консултант или друго радно ангажовано лице коме је одобрен приступ неком информатичком ресурсу Дома Здравља.

Корисник информатичких ресурса одговоран је за правилну употребу, тачност и сигурност података приликом коришћења информатичких ресурса Дома Здравља, односно лично је одговоран за остваривање својстава података у ИКТ систему Дома Здравља.

Дужности корисника информатичких ресурса
Члан 9.

Корисник не сме спроводити активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система Дома Здравља.

Корисник непреносиве радне станице је дужан да пословне податке смешта на одређене мрежне дискове на серверу Дома Здравља.

Изузетно од става 2. овог члана, због потребе посла, подаци се могу привремено сместити на локални диск непреносиве радне станице, ако се са тим сагласи непосредни руководилац корисника.

Корисник преносиве радне станице има право да привремено смешта пословне податке на локални диск преносиве радне станице, као и обавезу да уради копију докумената са локалног диска на мрежни диск сервера Дома Здравља.

Руководилац послова информационих система и технологије дужан је да дневно израђују резервне копије података са мрежних дискова Дома Здравља.

Корисник информатичких ресурса дужан је да поштује следећа правила безбедног и примереног коришћења информатичких ресурса и то:

1) да користи информатичке ресурсе искључиво у пословне сврхе;
2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власнишгво Дома Здравља и да могу бити предмет надгледања и прегледања;
3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4) безбедно чува своје лозинке, односно да их не одаје другим лицима;

5) пре сваког удаљавања од радне станице одјави се са система;
6) користи Апликације екстерне меморије на радној станици само уз одобрење Руководилац послова информационих система и технологије, а на основу образложеног предлога непосредног руководиоца;
7) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8) обезбеди сигурност података у складу са важећим прописима;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) не сме да на радној станици складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (Бекап) података у складу са прописаним процедурама;
13) користи Информациони систем Дома Здравља у складу са прописаним процедурама;
14) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
15) не сме да инсталира, модификује, искључује из рада или брише, заштитни, системски или апликативни софтвер;
16) да се уздржи од активности којима се изазива неоправдано оптерећење информатичких ресурса Дома Здравља, као и повећано ангажовање особља на одржавању тих ресурса;
17) не сме неовлашћено да објављује или преноси личне податке до којих је дошао коришћењем информатичких ресурса Дома Здравља;

Безбедносни профил корисника информатичких ресурса
Члан 10.

У зависности од описа задатака и послова радног места на које је распоређен, корисник информатичких ресурса, на предлог непосредног руководиоца, стиче одређена права приступа ИКТ систему Дома Здравља.

Администраторска овлашћења се могу добити само од Руководиоца послова информационих система и технологије, уз претходну сагласност директора Дома здравља.

Креирање лозинке
Члан 11.

Лозинка мора да садржи максимум осам карактера комбинованих од малих и великих слова и цифара.

Запослени - корисник информатичких ресурса је дужан да лозинку мења најмање једном у шест месеци.

Употреба корисничког налога
Члан 12.

Кориснички налог може употребљавати само корисник информатичких ресурса коме је исти издат.

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим Руководиоцу послова информационих система и технологије у случају подешавања радне станице.

Корисник информатичких ресурса је непосредно одговоран за активности које су реализоване на основу његовог корисничког налога.

Кориснички налози са администраторским овлашћењима користе се само за потребе неопходних интервенција којима се обезбеђује несметан рад информатичких ресурса (у даљем тексту: информатичке интервенције).

Употреба администраторског налога
Члан 13.

Администраторски налози свих пословних апликација, сервера база података и системских апликација за управљање мрежном опремом и уређајима за складиштење података чувају се и не смеју се злоупотребити.

Право коришћења администраторског налога има само Руководилац послова информационих система и технологије за потребе информатичких интервенција.

Поступци у случајевима сигурносних инцидената
Члан 14.

Корисник информатичких ресурса дужан је да, без одлагања, пријави непосредном руководиоцу свако уочавање или сумњу о наступању инцидента којим се угрожава сигурност ИКТ система.

Информацију о инциденту руководилац из става 1. овог члана дужан је да одмах проследи Руководиоцу послова информационих система и технологије. По пријави инцидента мора се поступати адекватно и ефикасно, а по хитном поступку у случајевима:

1) нарушавања исправности информација,
2) откривања вируса или грешака у функционисању апликација,
3) вишеструких покушаја неауторизованог приступа,
4) системских падова и престанка рада сервиса.

Руководилац послова информационих система и технологије дужан је да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести надлежни орган, у складу са законом којим се уређује информациона безбедност.

Заштита од малициозног софтвера
Члан 15.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена:

1) лиценцираног софтвера, односно забрана коришћења неауторизованог софтвера;
2) правила за заштиту од ризика приликом преузимања фајлова из екстерних извора (података, апликација и сл.).

Приликом преузимања фајлова из става 1. тачка 2) овог члана преносиви медији пре коришћења морају бити проверени на присуство вируса.

Ако се утврди да преносиви медиј садржи вирусе, врши се чишћење медија од вируса уз сагласност доносиоца медија.

Ризик од евентуалног губитка података приликом чишћења медија антивирусним софтвером, сноси доносилац медија.

Сигурност електронске поште
Члан 16.

У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

1) електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;
2) забрањено је коришћење електонске поште у приватне сврхе.

Поступање са преносивим медијима
Члан 17.

Преносиви медији који садрже податке морају да буду прописно обележени и пописани.

У случају брисања података који се налазе на преносивим медијима, потребно је обезбедити њихово неповратно брисање.

Преносиви медији из става 1. овог члана, пре стављања ван употребе, морају бити физички уништени.

Физичка сигурност информатичких ресурса
Члан 18.

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови:

1) сервери, сторици и комуникационо чвориште у просторијама Дома Здравља, морају бити смештени у посебној просторији (сервер соби), која испуњава стандарде противпожарне заштите и поседује редундантно напајање електричном струјом и адекватну климатизацију и у којој је забрањен приступ незапосленим лицима;
3) приступ сервер соби, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење Руководиоца послова информационих система и технологије;
4) радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;
5) просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
6) штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;
7) медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа;
8) за успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм.

Приступ ИКТ систему Дома здравља
Члан 19.

Руководилац послова информационих система и технологије, на основу прецизног писаног захтева непосредног руководиоца, додељује кориснику информатичког ресурса корисничко име, лозинку и привилегије, као и налог за електронску пошту.

Кориснику информатичких ресурса додељују се само привилегије које су неопходне за реализацију његових радних обавеза.

У случају престанка радног односа или радног ангажовања у Дому Здравља кориснику информатичког ресурса укида се право приступа ИКТ систему.

У случају одсуства са посла дуже од месец дана, кориснику информатичког ресурса се привремено укида право приступа ИКТ систему, до повратка на посао.

О престанку радног односа или радног ангажовања, одсуству са посла дуже од месец дана, као и о промени радног места корисника информатичких ресурса, непосредни руководилац је дужан да обавести Руководиоца послова информационих система и технологије ради укидања, односно измена приступних привилегија тог корисника.

Корисник информатичких ресурса, након престанка радног ангажовања у Дому Здравља, не сме да открива поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система.

Приступ ресурсима ИКТ система у Дому Здравља са удаљених локација, од стране запослених – корисника, у циљу обављања радних задатака, омогућен је путем заштитне VPN/интернет конекције.

Трећем лицу се могу одобрити права приступа ИКТ систему уз претходно склапање одговарајућег уговора, којим се прецизно дефинишу услови и обим права приступа, укључујући и све релевантне безбедносне захтеве.

Изузетно од става 8. овог члана, у случају неопходних и хитних послова, могу се одобрити права приступа трећем лицу по усменом налогу директора Дома Здравља, односно овлашћеног лица, о чему ће се накнадно, по завршетку посла, сачинити записник о оствареном приступу.

Ако се установи повреда уговорне обавезе или прекорачење овлашћења по основу уговора, одобрени приступ се одмах укида.

Инсталација и одржавање софтвера
Члан 20.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужен је Руководилац послова информационих система и технологије, који је дужан да поступа у складу са прописаним процедурама и упутствима.

Руководилац послова информационих система и технологије обезбеђује запосленом, односно ангажованом лицу, коришћење радне станице, (десктоп или лаптоп) са преинсталираним и правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачки програми (драјвери), пословно и развојно окружење, софтвер за вирусну заштиту, разне помоћне апликације), који је типски за све радне станице и који представља минимум потребан за обављање стандардних послова.

Руководилац послова информационих система и технологије врши оцену конзистентности траженог софтвера са постојећим инсталираним софтвером на предметној радној станици и уколико оцени да тражени софтвер неће угрозити или ометати рад, инсталираће захтевани софтвер, искључиво лиценцирану или бесплатну верзију.

Основна подешавања из става 2. овог члана су:

1) додељивање имена и TCP/IP адресе радној станици и њено придруживање домену;
2) подешавање станице клијента;
3) подешавање претраживача;
4) инсталација лиценцираног антивирус софтвера одобреног од стране Руководиоца послова информационих система и технологије;
5) инсталација званичног апликативног софтвера који одређене унутрашње јединице Дома Здравља користе у свом раду.

У случају да је кориснику потребно да се изврши инсталација одређеног специфичног софтвера на радној станици, непосредни руководилац подноси захтев електронским путем Руководиоцу послова информационих система и технологије.

Корисник информатичког ресурса дужан је да сваки проблем у функционисању оперативног система, маил клијента, претраживача, пословног софтвера аликативног софтвера, пријави непосредном руководиоцу који ову информацију прослеђује електронским путем Руководиоцу послова информационих система и технологије.

Проблем у функционисању антивирусног софтвера мора се пријавити без одлагања.

Руководилац послова информационих система и технологије дужан је да проблеме из става 6. и 7. овог члана отклони у најкраћем могућем року на локацији корисника, даљинском конекцијом ка радној станици или доношењем радне станице у Дома Здравља..

Члан 21.

У случају обраде података о личности приликом вршења надлежности и испуњења обавеза из овог правилника поступа се у складу са прописима које уређују заштиту података о личности.

Завршна одредба

Члан 22.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли Дома здравља.

Председник Управног одбора

Бошко Мишљеновић