На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/2016) и члана 26. Статута Дома здравља Обреновац, Управни одбор Дома здравља Обреновац на седници одржаној дана 16.05.2017. године доноси

ПРАВИЛНИК
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА ДОМА ЗДРАВЉА ОБРЕНОВАЦ

Предмет правилника

Члан 1.

Овим правилником ближе се дефинишу мере заштите информационо-комуникационих система у Дому здравља Обреновац (у даљем тексту Дом 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 правилника

Члан 2.

Циљеви доношења овог правилника су:

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

Обавезност правилника

Члан 3.

Овај правилник је обавезујући за све унутрашње јединице Дома здравља и за све кориснике информатичких ресурса, која користе информатичке ресурсе Дома здравља.

Непоступање запослених у Дому здравља, по одредбама овог правилника представља повреду радне обавезе због које се запосленом може отказати уговор о раду.

За праћење примене овог правилника надлежан је Одсек за информатику и комуникације Дома здравља (у даљем тексту: Одсек за ИК).

Појмови

Члан 4.

Поједини изрази употребљени у овим правилнику имају следеће значење:

1. **интегритет** је немогућност неовлашћене измене информација;

2. **расположивост** је доступност информација корисницима информатичких ресурса у обиму корисничког овлашћења;
3. **тајност** је обезбеђивање доступности информација само овлашћеним корисницима информатичких ресурса, као и немогућност приступа информацијама лица која немају таква овлашћења;
4. **администраторско овлашћење** је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;
5. **кориснички налог** јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно овлашћења корисника);
6. **администраторски налог** јесте јединствен налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и *уношење и измену свих осталих корисничких налога.*

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 сме 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 у Дому 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.

Корисник информатичких ресурса нема имовинска права над информатичким ресурсима Дома здравља.

Дужности корисника информатичких ресурса

Члан 9.

Корисник не сме да спроводи активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система Дома здравља.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне сврхе, а Дом здравља право да информатичке ресурсе повуче у било ком тренутку и у потпуности задржи све податке, без обавезе да их накнадно преда кориснику.

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 на екстерни диск.

Запослено лице у Одсеку информатике и у службама Дома здравља са администраторским овлашћењима (у даљем тексту: администратор), као и лица која су задужена за израду резервних копија, дужни су да дневно израђују резервне копије података са мрежних дискова и портала.

Запослено лице, корисник информатичких ресурса дужан је да поштује следећа правила безбедног и примереног коришћења информатичких ресурса, и то да:

1. користи информатичке ресурсе искључиво у пословне сврхе
2. прихвати да су сви подаци који се складиште, преносе или процесуирају у оквиру информатичких ресурса власништво 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. мења лозинке сагласно утврђеним правилима;
6. користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење Одсека за информатику, а на основу образложеног усменог или писаног предлога непосредног руководиоца;
7. захтев за инсталацију софтвера или хардвера подноси у писаној форми са образложењем и 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 дозволи приступ радној станици трећем лицу;
12. не сме да на радној станици складишти садржај који не служи у пословне сврхе;

13. израђује заштитне копије (backup) података у складу са прописаним процедурама;
14. користи Интернет и интернет имејл сервис у Дому здравља у складу са прописаним процедурама;
15. прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, израда мреже, покретање антивирусног програма и сл.) обавља у утврђено време.
16. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
17. прихвати да техничке сигурности (антивирусни програм, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему.
18. не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.
19. мора да најави нестанак ресурса неопходних за нормално функционисање ИКТ система Дома здравља.
20. у случају неочекиваних, изненадних оштећења насталих услед различитих радова у Дому здравља који су довели до угрожавања нормалног функционисања ИКТ система неопходно је обавестити Одсек информатике.
21. у случају промене послова или престанка радног ангажовања лице није овлашћено да износи и преноси информације трећем лицу везана за ИКТ систем 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 могу добити само лица која су задужена за одржавање информатичких ресурса у Дому здравља, уз претходну сагласност директора или помоћника директора односно лица задуженог за Одсек информатике у Дому здравља.

Креирање лозинке

Члан 11.

Лозинка мора да садржи минимум седам карактера комбинованих од малих и великих слова, цифара и специјалних знакова.

Ако корисник информатичких ресурса посумња да је друго лице открило његову лозинку дужан је да исту одмах промени.

Употреба корисничког налога

Члан 12.

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

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору у случају подешавања радне станице.

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

Администраторски налог омогућава приступ, контролу и администрацију информатичких ресурса али не и за измене активности коју је реализовао корисник информатичких ресурса.

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.

Право коришћења администраторског налога има само администратор за потребе информатичких интервенција.

Администраторском налогу додељено је право приступа, контроле и администрације информатичких ресурса али не и право измене активности коју је реализовао корисник информатичких ресурса.

Поступци у случајевима сигурносних инцидената

Члан 14.

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

Информацију у писаној форми са описом инцидента руководилац из става 1. овог члана дужан је да одмах проследи администратору, као и Одсеку за информатику Дома здравља.

По пријави инцидента мора се поступати адекватно и ефикасно, а по хитном поступку у случајевима:

1. нарушавања поверљивости информација,
2. откривање вируса или грешака у функционисању апликација,
3. вишеструких покушаја неауторизованих приступа,
4. системских падова и престанка рада сервиса.

Одсек информатике Дома здравља је дужан да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести надлежни орган дефинисан Законом о информационој безбедности („Службени гласник РС", број 6/2016) и директора Дома здравља.

Заштита од малициозног софтвера

Члан 15.

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

1. лиценцираног антивирусног 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 током чишћења медија антивирусним софтвером, сноси доносилац медија.

Пружаоци услуга

Члан 16.

У циљу сигурности коришћења услуга и сервиса пружаоци услуга морају поштовати следећа правила:

1. сва правила и норме предвиђена законом, уредбама, правилницима и другим законским актима Републике Србије
2. сва правила и норме предвиђена овим правилником и другим актима Дома здравља Обреновац
3. обавезност да обавесте Одсек информатике Дома здравља о инциденту у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности у писаној форми (извештај).
4. обавезност на поступање у складу са прописима којима је уређена област заштите тајних података;
5. ако је инцидент од интереса за јавност, треће лице нема право на објављивање већ упућује обавештење (извештај) Одсеку информатике Дома здравља који уз дозволу директора Дома здравља има право на објављивање.
6. ако је инцидент од интереса за јавност, треће лице има право објављивања инцидента само у складу са ставом 5. члан 11. Закона о информационој безбедности („Службени гласник РС", број 6/2016) .
7. ако је инцидент везан за извршење кривичних дела која се гоне по службеној дужности, треће лице је дужно да поступи по Закону о информационој безбедности („Службени гласник РС", број 6/2016) .
8. ако је инцидент везан са нарушавање права на заштиту података о личности, треће лице је дужно да поступи по Закону о информационој безбедности („Службени гласник РС", број 6/2016) .
9. одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су предвиђени овим правилником ближе ће се регулисати уговором са пружаоцем услуга и начелима овог правилника.

Сигурност електронске поште

Члан 17.

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

1. лозинка мора да садржи минимум седам карактера комбинованих од слова, цифара или специјалних знакова.
2. забрањен је приступ електронској пошти трећем лицу;
3. електронска пошта са прилозима не сме се отварати ако долази са сумњивих и

непознатих адреса, већ се мора пријавити администратору или избрисати;

4. забрањено је коришћење електронске поште у приватне сврхе;
5. избегавати постављање имејл адресе на другим веб презентацијама, блоговима, форумима, социјалним мрежама како не би била скенирана а потом искоришћена за слање СПАМ поште.
6. не смеју се користити приватни налози електронске поште у пословне сврхе;
7. програми који користе сервисе електронске поште морају се искључити када се рачунар не користи;
8. забрањено је чување корисничког имена и лозинке при пријави за преглед електронске поште на веб читачу и другим виндовс и андроид апликација.

Поступање са преносивим медијима

Члан 18.

Преносиви медији који садрже податке морају да буду прописно овележени и прописани.

У случају брисања података који се налазе на преносивим медијима, потребно је обезбедити њихово неповратно брисање (нпр. методом DiskWipe-a).

Физичка сигурност информатичких ресурса

Члан 19.

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

1. сервери, сторици (storage) и комуникациона чворишта у седишту Дома здравља морају бити смештени у посебној просторији (сервер сала) која испуњава стандарде противпожарне заштите (системи за сузбијање пожара, апарати за гашење пожара и сл.), поседује УПС и адекватну климатизацију а у оквиру могућности и систем контроле влажности ваздуха и температуре.
2. сервери, сторици (storage) и комуникациона чворишта морају бити смештени у адекватним просторијама, у којима је забрањен приступ незапосленим лицима;
3. приступ сервер сали, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење директора, помоћника директора, односно лица задуженог за Одсек информатике.
4. сервер сала мора да буде примерено обезбеђена и да буде онемогућен физички приступ и оштећење.
5. сервер сала мора бити адекватно обезбеђена након радног времена.
6. радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената
7. просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
8. штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;

9. медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа

Приступ ИКТ систему Дома здравља

Члан 20.

Приступ свим компонентама ИКТ система мора бити аутентификована.

Заснивањем радног односа или радног ангажовања корисник информатичких ресурса се обавезује на поштовање права, овлашћења и обавеза предвиђених Уговором о раду и овим правилником.

Непосредни руководилац је дужан да обавести запосленог или радно ангажовано лице о правима, овлашћењима и обавезама предвиђеним уговором и овим правилником.

Администратор, на основу прецизно писаног захтева непосредног руководиоца, додељује кориснику информационог 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.

О престанку радног односа или радног ангажовања, као и о промени радног места корисника информатичких ресурса, непосредни руководилац је дужан да обавести у писаној или електронској форми Одсек информатике 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 пословне тајне које су од значаја за информациону безбедност ИКТ система, у складу са Законом о тајности података.

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

Изузетак од става 8. овог члана, у случају неопходних и хитних послова могу се одобрити права приступа ИКТ систему трећем лицу по писаном 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 на основу уговора, одобрени приступ се одмах укида.

Инсталација и одржавање софтвера

Члан 21.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужен је администратор Одсека информатике, који је дужан да поступа у складу са прописаним процедурама и упутствима.

Одсек информатке обезбеђује запосленом, односно радно 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) и који представља минимум потребан за обављање стандардних послова.

Администратор Одсека информатике врши оцену конзистентности траженог софтвера са постојећим инсталираним софтверима на предметној радној станици и уколико оцени да тражени софтвер неће угрозити или ометати рад, инсталраће захтевани софтвер.

Основна подешавања из става 2. овог члана су:

1. додељивање имена и ТЦП/ИП адреса радној станици њеном придруживању домену или радној групи;
2. подешавање имејл клијената;
3. подешавање Веб претраживача (ТЦП/ИП адреса прокси сервера);
4. инсталација антивирусног софтвера одобреног од стране Одсека информатике;
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 површини, непосредни руководилац подноси електронским путем Одсеку информатике.

Корисник информатичких ресурса дужан је да сваки проблем у функционисању оперативног система, имејл клијента, Веб претраживача, пословног софтвера (MS Office или Open Office) и апликативног софтвера, пријави непосредном руководиоцу, који ову информацију пријављује у виду Налога за поправку и прослеђује Одсеку информатике.

Проблем у функционисању антивирусног и антиспајвер софтвера мора се пријавити без одлагања у виду Налога за поправку.

Администратор Одсека информатике је дужан да проблеме из ст.5 и ст.6 овог члана отклони у најкраћем могућем року у зависности од услова (нпр. временски услови, превоза и сл.) и по приоритетима које одређује информатичар у Дому здравља, на локацији корисника, даљинском конекцијом ка радној станици или доношењем радне станице у Одсек информатике.

Провера усклађености ИКТ система

Члан 22.

Оператор, администратор ИКТ система Дома здравља на основу члана 8. став 4 Закона о информационој безбедности („Службени гласник РС", број 6/2016) самостално или уз ангажовање спољних експерата врши проверу усклађености ИКТ система Дома здравља са предвиђеним мерама овим правилником и то најмање једном годишње и да о томе сачини извештај.

Центар за безбедност

Члан 23.

Дефинисано Законом о информационој безбедности („Службени гласник РС", број 6/2016), члан 19. Дом здравља је у обавези да формира сопствени центар за безбедност ИКТ система ради управљања инцидентима.

Формирани центар размењује информације са центрима других установа као и са националним ЦЕРТ-ом и са ЦЕРТОМ републичких органа, а по потреби и са другим организацијама.

Делокруг центра предвиђен је Законом о информационој безбедности („Службени гласник РС", број 6/2016), чланом 19.

Промена правилника

Члан 24.

Измене и допуне овог правилника морају бити усклађене и засноване на законима, којим се уређују одређени однос и правила пословања у Републици Србији и Дому здравља.

Завршна одредба

Члан 25.

Овај правилник ступа на снагу наредног дана од дана објављивања на интернет страници Дома здравља.

УПРАВНИ ОДБОР
ДОМА ЗДРАВЉА ОБРЕНОВАЦ
ПРЕДСЕДНИК

Горан Јовановић, дипл. инг.