На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16 и 94/17), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС“, бр. 94/2016) и члана 23. Статута Дома здравља „Др Верољуб Цакић“ Мајданпек директор Дома здравља „Др Верољуб Цакић“ Мајданпек дана 20. фебруара 2023. године доноси

Правилник о безбедности ИКТ система

Дом здравља „Др Верољуб Цакић“ Мајданпек

Верзија: прва, Датум почетка примене: 01.03.2023 године

Израдио: Предраг Брандушановић, администратор ИКТ система

Верификовао: Милан Милојковић дипл. инж. ИТ-а

Садржај

Члан 1. Намена

Намена Правилника је дефинисање правила и одговорности за утврђивање мера заштите у области информационе безбедности ИКТ система, њихово спровођење и контролу спровођења, ради достизања жељеног нивоа информационе безбедности пословних података у Дому здравља „Др Верољуб Цакић“ Мајданпек и спровођења обавеза које проистичу из Закона о информационој безбедности Републике Србије.

Члан 2. Примена

Одредбе овог Правилника обавезни су да поштују запослени у Дому здравља „Др Верољуб Цакић“ Мајданпек као и друга лица којима је омогућен приступ информационим ресурсима Дома здравља „Др Верољуб Цакић“ Мајданпек, а примењују се на сва технолошка решења, системе или опрему која у себи садржи или користи информационе технологије.

Члан 3. Информациона безбедност ИКТ система

Заштита информација подразумева обезбеђење следећих особина информације:

- поверљивост,
- интегритет,
- доступност,
- веродостојност и
- непорецивост.

Заштита информација се постиже применом одговарајућег скупа организационо-техничких мера и активности, укључујући надзор и контролу, обуку, радне процедуре, имплементацију техничких система заштите, примену физичких мера заштите, успостављање организационе структуре, примену софтверских алата или функција и слично.

Велики део информација које се креирају, чувају или размењују унутар Дома здравља „Др Верољуб Цакић“ Мајданпек налази се у електронском облику у оквиру ИКТ система Дома здравља „Др Верољуб Цакић“ Мајданпек.

У складу са дефиницијом термина „ИКТ система“ из Закона о информационој безбедности, Дом здравља „Др Верољуб Цакић“ Мајданпек поседује ИКТ систем.
У складу са дефиницијом термина „оператер ИКТ система“ из Закона о информационој безбедности, Дому здравља „Др Верољуб Цакић“ Мајданпек представља Оператера ИКТ система.

У складу са тачкама 3.) и 4.) члана 6. Закона о информационој безбедности, Дом здравља „Др Верољуб Цакић“ Мајданпек поседује и користи ИКТ систем од посебногзначаја.

Члан 4. Основна правила сигурности информација

При дефинисању организационо-техничких мера заштите података неопходно је поштовати следећа основна правила:

• разграничење дужности,

• правило „неопходно да зна“ (need-to-know),

• процена ризика,

• перманентна контрола и

• перманентно усавршање постојећих решења.

Члан 5. Разграничење дужности

Циљ разграничења дужности је да се спрече нежељене појаве и инциденти. Ово се може постићи расподелом задатака и доделом корисничких налога од којих је сваки за специфичан пословни процес.

Приступни параметри за сваки део информационог система чувају се у листи за чију се безбедност брине пројектант информационих система и програма и администратор информационих система и програма. Ажурну листу приступних параметара достављају Дому здравља „Др Верољуб Цакић“ Мајданпек приликом сваке измене, ради одвојеног чувања.

Члан 6. Правило „Неопходно да зна“(need-to-know)

Корисници могу да имају приступ само информацијама или функционалностима које су неопходне за правилно извршење њихових пословних задатака. Приступ информационим ресурсима мора бити експлицитно одобрен са јасном разликом између потребе да се подацима само приступи (*енг.* „read only“) и потребе да се подаци мењају (*енг.*„write“).

Члан 7. Процена ризика

Одговарајуће мере сигурности информација заснивају се на пословним захтевима, као и на проценама ризика, економској ефикасности и законским ограничењима. С обзиром на то да ниједан информациони систем никада не може да буде потпуно сигуран, треба проценити прихватљив ниво ризика након примене мера безбедности.

Члан 8. Перманентна контрола

Морају се вршити периодичне ревизије (минимум једном годишње) и провере како би се пратила општа усаглашеност са захтевима заштите информација, као и да би се открили сигурносне слабости или недостаци за које постоји сумња да могу утицати на ниво заштите информација.

Члан 9. Перманентно усавршање постојећих решења

Неопходно је вршити ревизију организационо-техничких решења у складу са променама у окружењу, након великих промена на информационом систему или у оквиру бизнис процеса, са циљем брзог и ефикасног реаговања и одржавања жељеног нивоа безбедности.

Члан 10. ИКТ систем

ИКТ систем чини више мањих ИКТ система (у даљем тексту ИКТ подсистеми).
ИКТ подсистеми раздвојени су на различите начине и по различитим критеријумима:

- на нивоу рачунарске мреже (одвојених фајерволом),
- на корисничком нивоу (ИКТ системе користе различита лица) и
- на апликативном нивоу (основна намена рачунара и апликација се разликује).

Члан 11. Мере заштите ИКТ система

Мере заштите ИКТ система морају да се усклађују са мерама прописаним Законом о информационој безбедности.

За усклађивање мера заштите одговорни су пројектант информационих система и програма и администратор информационих система и програма.

Члан 12. Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

Пројектант информационих система и програма установе је задужен и одговоран за управљање информационом безбедношћу ИКТ система

Дома здравља „Др Верољуб Цакић“ Мајданпек и прописивање мера заштите. У свим ИКТ подсистемима, примена мера заштите ИКТ система се мора спроводити у складу са Законом о информационој безбедности и актима Дома здравља „Др Верољуб Цакић“ Мајданпек.

Систем администратор је задужена да:

• прати примене које могу утицати на опште стање заштите информација у Дому здравља „Др Верољуб Цакић“ Мајданпек;

• прати и анализира сигурносне инциденте;

• додељује улоге у поступку заштите;

• координира и контролише примену мера заштите;

• обавештава надлежне државне органе о инцидентима у ИКТ Дома здравља „Др Верољуб Цакић“ Мајданпек, у складу са прописима.

Члан 13. Постизање безбедности рада на даљину и употребе мобилних уређаја

Термин мобилни уређај укључује: преносиве рачунаре, мобилне телефоне, есктерне меморијске медијуме (диск, УСБ кључ, и слично).
Радни однос за обављање послова ван просторија послодавца обухвата:

• Рад на даљину;
• Рад од куће.

Приликом удаљеног приступа ИКТ добрима неопходна је примена додатних мера заштите, укључујући аутентикацију на два нивоа, односно проверу приликом приступања ИКТ систему и проверу приликом приступања ИКТ подсистему. Приступање ИКТ систему и ИКТ подсистему могуће је ако корисник зна одговарајуће лозинке.

Приликом коришћења мобилних уређаја мора се обезбедити заштита пословних података и смањити ризике коришћења мобилних уређаја у незаштићеним окружењима (јавним местима, мрежама са непознатом или недовољном заштитом и слично).
За коришћење информатичких сервиса који су стандардно доступни преко интернета, а преко приватног мобилног уређаја запосленог, као на пример електронска пошта, нису потребне посебе сагласности.

Службени мобилни уређаји су у надлежности Дома здравља „Др Верољуб Цакић“ Мајданпек и издају се запосленима ради коришћења приликом обављања службених обавеза.
Приликом коришћења бежичних мрежа морају се примењивати мере заштите бежичних мрежа предложене од стране Пројектанта информационих система и програма установе.

Члан 14. Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност

Сваки нови запослени може добити приступ информационим и техничким ресурсима тек пошто прође одговарајућу обуку за рад, упозна се са прихватљивом употребом информатичких ресурса.

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и у примени код Дома здравља „Др Верољуб Цакић“ Мајданпек.

Члан 15. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Приликом престанка радног односа запосленог, преласка запосленог на друге послове или престанка сарадње са пословним партнером, потребно је да надлежни руководилац информише запосленог, односно пословног партнера, о свим захтевима везаним за заштиту информација и подсети га на законске обавезе из области заштите информација.
Измена одговорности или промена послова морају се третирати као престанак тренутних одговорности, а нове одговорности разматрати као да се ради о запошљавању и закључењу новог уговора или споразума.

За поступања приликом престанка запослења или ангажовања задужен је Пројектант информационих система и програма установе, који предузима следеће активности:

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату;
- прегледа све налоге и приступе систему који су били доступни запосленом;
- преузима од запосленог електронске и друге мобилне уређаје;
- проверава враћене мобилне уређаје и уређаје за преношење података;
- даје налог за укидање налога електронске поште и свих других права приступа систему Дома здравља „Др Верољуб Цакић“ Мајданпек на дан престанка радног односа или другог основа ангажовања бившег запосленог;
- прегледа све налоге за приступ одлазећег запосленог и прикупља приступне шифре и кодове са циљем укидања/промене истих на дан одласка;
- преузима картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Дома здравља „Др Верољуб Цакић“ Мајданпек.

Члан 16. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Пројектант информационих система и програма установе води евиденцију о ИКТ добарима. Дом здравља „Др Верољуб Цакић“ Мајданпек мора да:

• на ИКТ добра примењује мере заштите прописне Законом о информационој безбедности и актима Дома здравља „Др Верољуб Цакић“ Мајданпек

• да мере заштите ИКТ добара примењује у складу са степеном осетљивости и критичности тих добара, узимајући у обзир могуће последице нарушавања поверљивости, интегритета и расположивости добара

Сви запослени, извођачи радова и пословни партнери морају бити на одговарајући начин упознати са правилима и одговорностима за коришћење информација и опреме за процесирање информација и у обавези су да их се придржавају.

Члан 17. Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности

Мере заштите података који су, у складу са законом који уређује област тајности података, означени као тајни, одређују се у складу са прописима који регулишу ову област.
Избор и ниво примене мера заштите података се заснива на процени ризика, потреби за превенцијом ризика и отклањању последица ризика који се остварио, укључујући све врсте ванредних околности.

Дом здравља „Др Верољуб Цакић“ Мајданпек својим активностима генерише податке који су доступни јавности на увид. Откривање таквих података не изазива никакву штету. Подаци који су заштићени су лични подаци лица укључених у процесе рада здравствене установе.

Члан 18. Заштита носача података

У циљу спречавања неовлашћеног приступа, модификовања, уклањања или уништења података постоје одговарајуће оперативне процедуре за заштиту, рад, транспорт и складиштење докумената и носилаца података (медијума за смештај података као дискови, екстерне меморије, “CD”, “DVD” медијуми, документације о ИКТ добрима и системима и слично), као и процедуре за безбедно брисање података са носилаца података.
За размену информација ограниченог приступа морају се стандардизовати и користити одговарајуће техничке мере заштите и доследно их примењивати у свим деловима Дома здравља „Др Верољуб Цакић“ Мајданпек.

Обавезно је минимизовати коришћења преносних медијума. Пре коришћења преносни носачи информација морају се подвргнути провери средствима за заштиту од злонамерног софтвера. За коришћење преносних медијума потребна је дозвола Вишег стручног сарадника за информациону подршку, статистику и анализу здравствених установа.
Обавезно је поуздано уништење података са носача података који се не користе више од годину дана. У случају немогућности поузданог уништења података мора се обавити физичко уништење носача.

Приликом рада са носиоцима података корисници се придржавају следеће процедуре:

-Корисник је дужан да процени поузданост носиоца података – поуздани носиоц је онај који је обезбедио Дом здравља „Др Верољуб Цакић“ Мајданпек. Сви носиоци података из других извора морају да се проследе на проверу Администратору информационих сустема. После овакве провере може се приступити раду са носиоцем података.

-Корисник у току рада мора да има надзор над носиоцем података у сваком тренутку. Не сме се остављати носиоц података доступан другим лицима, како би се спречила могућност да дође до читања или уписа података од стране неовлашћеног лица.

- По завршетку рада корисник одјављује носиоц података са система и лично води рачуна о безбедности носиоца података или га предаје на чување Администратору информационих сустема установе.

Заштита носиоца података:

-Корисник је дужан да чува носиоце података на безбедном месту које је под његовим надзором или поверити чување Администратору информационих сустема установе.

-Проверу поседовања носиоца података дужан је да обавља на дневном нивоу.

-У случају нестанка носиоца података у најкраћем року обавештава Администратора информационих сустема установе.

Транспорт нициоца података:
-У случају да се носиоц података износи из просторија Дома здравља „Др Верољуб Цакић“ Мајданпек корисник има обавезу да обезбеди сигурност истог.

-Корисник мора да зна које податке транспортује на носиоцу података, како би у случају нестанка носиоца података могло да се процени да ли постоји и колики је ризик по безбедност информационог система.

-У случају нестанка носиоца података приликом транспорта корисник је дужан да у најкраћем року обавести о нестанку Администратора информационих сустема установе.

Складиштење носиоца података:

-Корисник је у обавези да носиоц података чува на безбедном, закључаном месту које је обезбеђено од могућности приступа неовлашћених лица.

-Безбедност места за складиштење корисник проверава свакодневно.

О складиштењу носиоца података који нису додељени кориснику брине се Администратор информационих сустема установе.

Брисање носиоца података:

-Корисник је у обавези да приликом брисања података обезбеди да се податак избрише и из привремене меморије рачунара.

-Носиоц података који није предвиђен за брисање се уништава физички када више није потребан.

-Носиоц података који више није потребан кориснику, а који се не брише или уништава предаје се Администратору информационих сустема установе.

Члан 19. Ограничење приступа подацима и средствима за обраду података

Корисницима се додељују минимална права приступа и привилегије за приступ ИКТ добрима, потребна за обављање пословних задатака, укључујући у то и приступ рачунарској мрежи и мрежним ресурсима.

Ограничење приступа подразумева:

• физичку контролу приступа (браве)

• административно ограничење приступа (раздвајање надлежности)

• техничка контрола приступа (корисници система са дефинисаним врстама приступа у оквиру мрежних уређаја, логови догађаја у систему, софтвер за заштиту од злонамерног софтвера, бекап података и слично).

Ограничење приступа врши се у складу са улогом корисника ИКТ система. Све методе контроле приступа морају се разматрати заједно. Приступ се ограничава уређајима које корисник користи за приступ информационим и техничким ресурсима. Контрола минимално подразумева аутентикацију корисника и контролу приступа информационим услугама.

Члан 20. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Власник информација је служба Дома здравља „Др Верољуб Цакић“ Мајданпек и онауправља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.
Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Додељивање привилегованих (администраторских) права на приступ врши се на основу Уговора о раду.

Привилегована права на приступ која треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности. Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора. Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора. Шифре за приступ општим корисничким идентификаторима администратора се мењају променом корисника.

Дом здравља „Др Верољуб Цакић“ Мајданпек једном годишње врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај запослења).

Запосленима, другим радно ангажованим и екстерним корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.
Корисници приликом напуштања радног места, морају предузети мере за заштиту радног места од неовлашћеног приступа. У току рада корисници морају да поштују правила „чистог стола“и „чистог екрана“ што значи да се напуштањем радног места, то место мора очистити од докумената, а рачунар закључати тако да је обавезна наредна операција пријава на систем (уношење корисничког налога и шифре).

Корисничко име и лозинке се морају користити као стандардно средство за верификацију идентитета корисника пре давања приступа информационом систему или услузи, у складу са овлашћењима корисника.

Рад корисника у оквиру оперативног система обавља се под корисничким налозима са ограниченим правима. Приступ оперативном систему омогућен је корисницима тек након што прођу процедуре идентификације и аутентификације.

Члан 21. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Аутентификације корисника којима је одобрен приступ систему врши се путем јединственог корисничког имена и шифре.

Сви корисници су дужни да:

• корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;

• избегавају чување корисничког имена и шифре у писаном облику;

• промене шифру када примете да постоји било какав наговештај могућег компромитовања.

Шифре морају да:

• Садрже најмање 6 алфанумеричких карактера;

• Садрже најмање једну цифру.

Шифре не заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и не смеју садржати више од 3 узастопна идентична бројчана или словна знака. Корисници су дужни да привремене шифре промене приликом првог пријављивања.

Члан 22. Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Дом здравља „Др Верољуб Цакић“ Мајданпек у свом пословању нема података које треба да заштити криптографски. Област у којој се користи криптографска заштита је дигитални потпис ради потврде аутентичности документа. Дигитални потпис се користи у складу са правилима издаваоца дигиталног сертификата.

Члан 23. Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему

Неопходно је спречити неовлашћен физички приступ објектима, просторима, просторијама у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему.

Члан 24. Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем

Неопходно је заштитити средства која чине ИКТ систем од губитка, оштећења, крађе или другог облика угрожавања безбедности. У циљу заштите средстава, неопходно је водити рачуна о постављању средстава на безбедна места, елиминисати непотребан приступ у простор у коме се налазе, вршити редовне провере заштићености средстава од крађа, пожара, и других претњи и пратити услове околине (температура, влажност и др.) који би могли негативно да утичу на рад средстава.

Средства треба да буду заштићена у случају поремећаја у дистрибуцији електричне енергије, телекомуникационих капацитета, воде, вентилације обезбеђивањем алтернативних решења која омогућују наставак рада ИКТ система.

Измештање имовине ИКТ подсистема може да се врши само уз претходно одобрење овлашћеног лица, уз примену безбедносних механизама, узимајући у обзир различите ризике приликом рада изван просторија организације.

Области приступа где неовлашћена лица могу ући у службене просторије, треба контролисати, како би се избегао неовлашћени приступ опреми ИКТ система.
Информациони и технички ресурси се морају физички заштитити да би се спречио губитак, оштећење, крађа или други негативни утицаји, који могу представљати претњу.
Техничка средства се морају одржавати у складу са експлоатационом документацијом и упутством произвођача како би се осигурала непрекидна расположивост и интегритет података.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

1. Све осетљиве и поверљиве информације у штампаном или електронском облику запослени морају одложити на сигурно место на крају радног дана или када нису присутни на свом радном месту.
2. Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана.
3. Ормари и фиоке у којима се чувају поверљиви подаци морају бити закључани када се не користе, а кључеви не смеју бити остављени на приступачном месту без надзора.
4. Носачи података као што су дискови и flash меморија морају бити одложени и закључани.
5. Шифре за приступ не смеју бити написане и остављене на приступачном месту.
6. Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.
7. Материјал који је намењен за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

Након оштећења уређаја који садрже критичне или поверљиве податке, неопходно је спровести процену ризика да дође до одлива поверљивих података приликом предаје уређаја ради одржавања екстерним организацијама. У случају доношења одлуке о немогућности предаје уређаја, уређај се уништава уз састављање одговарајућих докумената, након чега се врши његова замена у складу са утврђеним стандардима.

Члан 25. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, дефинишу се процедуре за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевима измештања делова ИКТ система.

Дома здравља „Др Верољуб Цакић“ Мајданпек користи радне процедуре које садрже инструкције за детаљно извршење следећих послова:

а) инсталација и конфигурација система;

Системски софтвер сервера инсталира и конфигурише фирма коју Дом здравља „Др Верољуб Цакић“ Мајданпек изабере за партнера. Инсталације се обављају уз проверу Пројектанта информационих система и програма установе.
База података се инсталира на серверу установе у фолдеру насловљеном са Базе. За инсталацију је задужен Администратор информационих система и технологија установе.

б) обраду и поступање са информацијама (аутоматски и мануелно);

Обрада и поступање са информацијама се обавља коришћењем десктоп апликације установе. Десктоп апликација својим подешавањем корисницима дозвољава рад само над оним делом података који су додељени том кориснику. Путем десктоп апликације корисник не може да види податке ван својих ингеренција.

в) израда резервних копија;

-База података, односно њен садржај се прави на дневном нивоу из окружења SQL Server Management Studio/ MPEKDB/Databases/(naziv baze)/ Tasks / Back up . Фајл настао овим поступком остаје на серверу, а као додатна мера копира се на хард диск намењен прављењу резервних копија или се нарезује на двд дискове. За копирање базе података задужен је Администратор информационих система и технологија установе.

-Апликација установе се копира периодично по потреби после уношења измена на програму. Копира се садржај фолдера на серверу на путањи E:\NexTData\(naziv programa). Садржај се копира се на хард диск намењен прављењу резервних копија или се нарезује на двд дискове. За копирање апликације задужен је Администратор информационихб система и технологија установе..

-Веб презентација Дома здравља „Др Верољуб Цакић“ Мајданпек се налази на веб адреси http://www.dzmpek.org.rs/ Овој адреси приступа параметрима који су наведени у документу „Параметри за приступ Информационим ресурсима Дома здравља „Др Верољуб Цакић“ Мајданпек “.
На порталу Ц панел у одељку Бекап се покреће прављење бекапа веб презентације. Формирани фајл се са овог портала копира на информациони ситем Дома здравља „Др Верољуб Цакић“ Мајданпек. Затим се тај фајл копира на хард диск намењен прављењу резервних копија или се нарезује на двд дискове.За копирање веб апрезентације Дом здравља „Др Верољуб Цакић“ Мајданпек задужен је Пројектант информационих система и програма установе.

-Електронска пошта за сваког корисника се налази на његовом службеном рачунару. За резервну копију своје електронске поште задужен је сваки корисник лично. Резервна копија електронске поште прави се најмање једном месечно. За прављење копије треба копирати садржај фолдера C:\Users\ime.usera \Documents\Outlook Files. Сваки корисник који је добио од установе УСБ меморију на коју снима садржај електронске поште, у случају недовољно меморије за нови бекап, треба обрисати стари бекап.

-Радна документа са корисничких рачунара: у свом раду корисници израђују радне фајлове који су њихова лична олакшица у раду и као такви нису од вишег интереса за установу. Радне фајлове корисници треба да групишу у фолдере у оквиру путање C:\Users\ime.usera \Documents или на десктопу. Копију својих радних фајлова корисници праве лично, минимално једном месечно. Фајлове копирају корисници на УСБ меморију добијену од установе.

г) инструкција за поступање у случају грешке или у другим ванредним ситуацијама која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција

У случају грешке на информационом систему корисник бележи датум и време настајања грешке, место на апликацији на којем је настао проблем, копира поруку коју је јавио систем у електронској форми или прави писану забелешку поруке, обавештава Администратора информационих система и технологија установе о случају грешке.

д) утврђивање листе контаката за подршку и ескалацију (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа.

У случају неочекиваних оперативних или техничких потешкоћа подршка се тражи од Администратора информационих система и технологија установе.
Екстерна подршка за случај
проблема на системском софтверу :
podrska@bitths.rs
за проблеме на веб презентацији:
hosting@oriontelekom.rs

ђ) процедуре за поновно покретање система и опоравак, које се користе у случају отказа система;

У случају отказивања системског софтвера тражи се екстерна подршка од партнера Дома здравља „Др Верољуб Цакић“ Мајданпек.

У случају отказивања апликације и базе података, ради се резервна копија базе података и резервна копија апликације са путање E:\NexTData\(naziv programa). Ове копије служе за даљу анализу насталог проблема. Преко постојеће базе података на серверу се кроз програм SQL Server Management Studio ради ресторирање последње верзије базе из бекапа.
За апликацију се распакива последња верзија резервне копије апликације и копира на путању E:\NexTData\(naziv programa) на серверу. После ових поступака рестартује се сервер и врши провера информационог система. Корисници при првом приступању апликацији проверавају последње податке које су унели и извештавају о успеху или неуспеху Администратора информационих системаи технологија установе.

За усвајање, измене и допуне радних процедура овлашћен је Администратор информационих системаи технологија установе.
Коришћење ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе система. Периодично се спроводе следеће активности:

а) брисање застарелих података;
б) повлачење из употребе апликација, система, база података или окружења;
в) оптимизација серије процеса и распореда;
г) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису критичне за пословање.

Окружења за развој, испитивање и рад су међусобно раздвојена, како би се смањио ризик од неовлашћеног приступа или промена у радном окружењу.

а) преношење софтвера из развојног статуса у оперативни статус обавља Администратора информационих системаи технологија установе;
б) развојни и оперативни софтвери треба да се извршавају на различитим системима или рачунарским процесорима, као и у различитим доменима или директоријумима;

в) промене у оперативним системима и апликацијама треба испитивати у окружењу за испитивање или режиму одржавања пре него што се примене на оперативне системе;

г) испитивање не треба да се ради на оперативним системима, осим у изузетним околностима;

д) компајлери, едитори и други развојни алати или системски помоћни програми не треба да буду доступни из оперативних система, ако се то не захтева;

ђ) да би се смањио ризик од грешке, корисници треба да примењују различите корисничке профиле за оперативне и системе за испитивање, а менији треба да приказују одговарајуће идентификационе поруке;

е) осетљиве податке не треба копирати у системско развојно окружење, осим ако нису обезбеђене еквивалентне контроле за систем за испитивање.

За обезбеђивање исправног и безбедног функционисања средстава за обраду података и примену радних процедура задужен је Пројектант информационих система и програма установе.

Члан 26. Заштита података и средства за обраду података од злонамерног софтвера

Злонамерни софтвер представља значајну претњу за ІКТ систем, јер може да доведе до оштећења или губитка података. Одговарајући антивирусни системи се морају применити на свим нивоима (радне станице / лаптопови, сервери, електронска пошта, приступ интернету) да би се омогућила ефикасна заштита.

1. Антивирус системи морају да се инсталирају само од стране овлашћеног особља и на начин који неће омогућити корисницима да их уклоне или да им промене конфигурацију.

2. Антивирус систем мора да омогући корисницима да у потпуности скенирају своје радне станице / лаптопове или преносиве медијуме, односно да се то врши аутоматски.

3. Антивирус систем мора да буде тако конфигурисан да може да скенира податке када се они уносе у компјутер. Овај поступак ће обухватити скенирање сваког фајла, идентификовање злонамерног кода, уклањање или стављање истих у карантин, ако уклањање није могуће. Ако антивирус систем не може да уклони малвер или да га стави у карантин, онда заражени објекат/фајл мора да се пошаље испоручиоцу антивируса на додатну анализу.

4. Фајлови који долазе са Интернета, поруке путем електронске поште и прилози, као и сви преносиви медијуми за складиштење података (као што су USB меморије, екстерни хард дискови, CD-ови / DVD-јеви, итд.) морају се аутоматски скенирати пре него што се прикључе у ИКТ систем.

5. Антивирус систем мора редовно аутоматски да се ажурира и такав поступак треба да буде транспарентан крајњем кориснику.

6. Строго је забрањено поседовање, дистрибуција и развој злонамерног софтвера.

Управљање и обнављање средстава за заштиту од злонамерног софтвера врши се централизовано, од стране Пројектанта информационих система и програма установе и Администратора информационих системаи технологија установе.

Анализирати случајеве продирања и имплементације злонамерног софтвера у оквиру мера за управљање инцидентима информационе безбедности.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Администратору информационих системаи технологија установе.

У циљу заштите од упада у ИКТ систем, Пројектанта информационих система и програма установе и Администратор информационих системаи технологија установе су дужни да одржавају систем за спречавање упада. Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе ИнтернетаПројектант информационих система и програма установе може укинути приступ.

Члан 27. Заштита од губитка података

Дом здравља „Др Верољуб Цакић“ Мајданпек врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.
Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.
Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих и log фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

За чување заштитних копија користе се екстерни хард дискови и CD/DVD медији.

Администратор информационих система и технологија установе извршава следеће задатке:

-процењује осетљиве и критичне податке за које је потребно правити резервне копије;
-креира план прављења резервних копија;
-прави заштитне копије серверског оперативног система, конфигурационих фајлова, апликације, и базе података;
-верификује успешно прављење резервних копија;
-води евиденцију урађених резервних копија;
-одлаже копије на безбедно место;
-тестира исправност резервних копија и процедуре за прављење заштитних копија;
-рестаурира податке са резервних копија.

Израда резервних копија, поступак приликом израде и учесталост израде резервних копија наведена је у члану 25 под тачком в)

-резервне копије треба да одражавају пословне потребе организације и критичност тих информација по континуитет пословања организације;
-треба их складиштити на локацији на довољној удаљености, како би се избегло свако оштећење на главној локацији;
-резервним копијама информација треба дати одговарајући ниво физичке заштите и заштите од утицаја околине који је доследан мерилима која се примењују на главној локацији;
-медијуме са резервним копијама треба редовно проверавати, ради сигурности њихове употребе у ванредним ситуацијама и када је то неопходно;
-у ситуацијама у којима је важна поверљивост, резервне копије треба заштитити помоћу шифровања.

За заштиту од губитка података одговорни су Пројектант информационих система и програма установе и Администратор информационих система и технологија установе.

Члан 28. Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Обезбедити евидентирање свих активности корисника, администратора, оператера, порука о процесима, грешкама, промени конфигурације система и слично. Уколико другим нормативним актом није другачије прописано, минималан рок обавезног чувања наведене евиденције је једна година.

Средства за записивање и записи треба да буду заштићени од неовлашћеног приступа и промене. Записи се редовно преиспитују у циљу заштите.
За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужен су Пројектант информационих система и програма установе и Администратор информационих система и технологија установе.

Члан 29. Обезбеђивање интегритета софтвера и оперативних система

У циљу одржавања исправности софтвера врше се мере отклањања слабих тачака софтвера. Отклањање слабих тачака софтвера се постиже редовним инсталирањем нових верзија софтвера. Ажурирање оперативних ситема и другог опште-системског и апликативног софтвера врши Администратор информационих система и технологија установе.

Члан 30. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

У циљу правовременог и ефикасног реаговања на објављене и уочене слабе тачке софтвера се предузимају мере за контролу заштићености средстава за обраду, чување и предају информација.
Контрола заштићености се врши на следећи начин:

• периодичном анализом заштићености помоћу скенерања безбедносним алатима/софтверима

• мониторингом заштићености

• анализом конфигурационих фајлова средстава за обраду, чување и пренос информација

Подаци о слабим тачкама софтверских решења редовно се обнављају са сајтова произвођача конкретних решења. Уочене слабе тачке средстава за обраду, чување и пренос информација отклањају се помоћу нових верзија софтвера („update“) или применом препоручених конфигурација које нуде произвођачи софтвера.

Све обављане активности контроле заштићености и уклањања слабих тачака се документују.

Члан 31. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Приликом спровођења контроле ИКТ система, Дом здравља „Др Верољуб Цакић“ Мајданпек обезбеђује да предузете активности имају што мањи утицај на функционисање система, тако што планира адекватно време спровођења ревизије и редослед активности који не ометају пословне процесе унутар ИКТ система.

Члан 32.Заштита података у комуникационим мрежама укључујући уређаје и водове

У циљу заштите података у комуникационим мрежама, уређајима и водовима врши се њихова контрола и заштита од неовлашћеног приступа, дефинише одговорност за управљање мрежном опремом, одговорност за рад мреже, посебне контроле за заштиту поверљивости и интегритета података који пролазе путем јавних или бежичних мрежа.
За спровођење редовних провера постојања адекватне безбедности мрежних сервиса ангажују се фирме које се баве одржавањем мрежа рачунара.
Комуникационим мрежама адекватно управљати и контролисати их, како би се оне заштитиле од претњи, да би се одржала сигурност система и апликација које користе мрежу, укључујући и заштиту информације које су у протоку.
Приликом закључивања уговора о мрежним услугама, за све мрежне услуге треба идентификовати ризике и узети у обзир елементе заштите информација да се ризици минимизују.

Члан 33. Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система

Заштита података који се преносе комуникационим средствима унутар Дома здравља „Др Верољуб Цакић“ Мајданпек, између установе и лица ван установе, обезбеђује се утврђивањем одговарајућих правила, процедура и применом адекватнихконтрола.

Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са успостављеним процедурама и адекватним контролама над спровођењем истих. Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

Правила коришћења Интернета

Приступ садржајима на Интернету је дозвољен искључиво за пословне намене. На мрежи је омогућено надгледање, односно користи се поступак периодичне ревизије и контролисања логовања, како на пријему тако и на слању.

Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом.

Члан 34. Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Информациона и техничка решења обухватају оперативне системе, инфраструктуру, пословне апликације, ИТ услуге других лица, готове софтверске пакете и хардвер.

За увођење новог система за обраду информација мора се претходно обезбедити:

• сагласност Пројектанта информационих система и програма установе, статистику и анализу здравствених установа, којом се потврђује да имплементација новог система не нарушава постојећи систем заштите информација и

• сагласност овлашћеног лица Дома здравља „Др Верољуб Цакић“ Мајданпек којомсе потврђује да имплементација новог система не нарушава функционисање и неопходне перформансе ИКТ система.

Дома здравља „Др Верољуб Цакић“ Мајданпек обавезан је да контролише промене везане за информациона добра ИКТ система. Информациона добра као што су хардвер,

комуникациона инфраструктура, системски софтвер и апликативни софтвер морају бити предмет строге контроле управљања променама.

Примена мера заштита информација је обавезна током целог животног века информационих и техничких решења у:

• фази пројектовања,

• фази обезбеђења буџета,

• фази поступка набавке,

• фази поступка уговарања,

• фази експолатације,

• фази поступка измене или унапређења постојећег система и

• фази поступка престанка са коришћењем система.

Пројектант информационих система и програма установе, статистику и анализу здравствених установа проверава примену мера заштите у свим наведеним фазама.

Члан 35. Заштита података који се користе за потребе тестирања ИКТ система односно делова система

За потребе тестирања ИКТ система односно делова система Власник ИКТ система користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.
Апликације и софтвер оперативног система имплементирати тек после успешно спроведеног тестирања, којим треба обухвати проверу применљивости, сигурности, утицаја на друге системе и погодности за коришћење.

Током тестирања избегавати коришћење продукционих база података које садрже осетљиве информације. Ако се за сврху испитивања користе информације о личности или неке друге осетљиве информације, неопходно је применити мере заштите информација као на стварним, продукционим системима у складу са прописима и овлашћењима.

Приступ изворном програмском коду и припадајућим информацијама строго контролисати, како би се спречило увођење недокументованих и неауторизованих функција, као и да би се избегле ненамерне промене.

Члан 36. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Размену информација и софтвера са пословним партнерима заснивати на званичној политици размене, регулисане одговарајућим уговорима, односно споразумима.

Коришћење екстерних организација за управљање информационим и техничким ресурсима представља сигурносни ризик, те је неопходно унапред извршити процену ризика, припремити одговарајуће мере заштите.

Ангажовани од стране Пословног партнера не могу имати права администрирања која су потребна за промену параметара аутентификације, ауторизације и права приступа. Током пружања услуга, ангажовани од стране Пословног партнера, морају имати минимална права потребна за обављање послова, а која нису у супротности са претходним ограничењима. Морају се применити следеће мере:

• употреба персонализованих корисничких налога (име и презиме);

• непходно је увек прво приступити приступној тачки на којој се бележе све активности у дневницима (логовима).

Мере заштите које се примењују приликом приступа лица запослених преко фирми које пружају услуге изнајмљивања људских ресурса идентичне су мерама заштите које се примењују на запослене у установи. У свим фазама рада са информационим и техничким ресурсима, треба обезбедити могућност контроле и увида у активности ангажованих екстерних организација.

Члан 37. Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга

У циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, неопходно је успоставити механизме надзора над пружањем услуга. Пројектант информационих система и програма установе задужен је за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности.

Члан 38. Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама

Власник ИКТ система утврђује:

• одговорно лица задужено за превенцију и реаговање је Пројектант информационих система и програма установе

• план поступања у случају опасности од настанка безбедносних инцидената или настанка безбедносних инцидената,

• обавезе вођења евиденције о предузетим активностима,

• обавезе извештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.

Сви запослени и пружаоци услуга су обавезни да одговорном лицу, задуженом за превенцију и реаговање из става 1. овог члана, без одлагања пријављују безбедносне слабости, претње и инциденте у ИКТ систему.

Власник ИКТ система одређује Пројектанта информационих система и програма установе као лице одговорно за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности.

Одговорно лице примењује поступак идентификације, прикупљања и чувања информација које могу да послуже као доказ ради покретања дисциплинског, прекршајног или кривичног поступка.

У циљу правовременог утврђивања прекршаја у области информационе безбедности врши се контрола догађаја у оперативним и апликативних системима, уређајима и окружењу, уз обавезно вођење дневника догађаја.

Обавезна је регистрација:

• активности корисника које се тичу приступа оперативним и апликативним системима, информационим ресурсима и мрежним сервисима,

• активности корисника које се тичу рада са преносним носачима информација на њиховим радним местима и

• активности на измени подешавања средстава за обраду, чување и пренос информација, средстава за заштиту информација и права приступа корисника.

Морају се предвидети механизми за заштиту дневника (лога) догађаја од препуњавања, неовлашћеног прегледања и уношења измена.

Дневници (логови) догађаја се редовно анализирају од стране Пројектанта информационих система и програма установе. Након оштећења уређаја који садрже критичне или поверљиве податке, неопходно је спровести процену ризика да дође до одлива поверљивих података приликом предаје уређаја ради одржавања екстерним организацијама. У случају доношења одлуке о немогућности предаје уређаја, уређај се уништава уз састављање одговарајућих докумената, након чега се врши његова замена у складу са утврђеним стандардима. Све запослене, извођаче радова и екстерне кориснике треба

упознати са процедурама за извештавање о догађајима и слабостима које могу имати последице по пословање.

Члан 39. Посебна обавеза Дома здравља „Др Верољуб Цакић“ Мајданпек

Обавеза Дома здравља „Др Верољуб Цакић“ Мајданпек је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Правилника обезбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Дома здравља „Др Верољуб Цакић“ Мајданпек.

Члан 40. Одговорности и препоруке

За управљање информационом безбедношћу у складу са Законом о информационој безбедности на нивоу ИКТ система установе задужен је Пројектант информационих система и програма установе.

Одговорност за примену мера заштите ИКТ система дефинисаних Законом о информационој безбедности, одговоран је Дом здравља „Др Верољуб Цакић“ Мајданпек. За израду, измене и допуне у тумачење одредби овог Правилника одговоран је Пројектант информационих система и програма установе.

Члан 41. Ступање на снагу Акта о безбедности

Овај правилник ступа на снагу 8.(осмог) дана од дана доношења,а даном доношења објављује се на Огласн табли и интернет презентацији Дома здравља „Др Верољуб Цакић“ Мајданпек.

ДИРЕКТОР

Драган Фудуловић

Број:

Мајданпек, 20.фебруар 2023. године