На основу члана 8. став 1 и члана 6б, став 2. Закона о информационој безбедности („Службени гласник РС”, број 6/16, 94/17 и 77/19), чл. 2. и 3. 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 94/16), , доноси

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

Овим Актом су обухваћене све мере заштите предвиђене Законом о информационој безбедности, Уредбом о ближем садржају акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја.

Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буде заштићен од неовлашћеног приступа. У заштиту ИКТ система спада заштита хардвера, софтвера, мреже, целокупног сајбер простора од различитих злоупотреба хакерским упадом у ИКТ систем. ИКТ систем мора да буде заштићен да би се задржао интегритет, расположивост, аутентичност и непоречност података да би тај систем функционисао како је предвиђено и под контролом овалшећених лица. Закон о заштити подата о личности нагласио је важност ефикасне заштите информација. Дакле управљање ИКТ инфраструктуром мора бити у складу и са Законом о заштити личних података, посебно када је реч о обрађивачу података.

Овај Акт је стратешки документ који сетом прилагођених и стандардних процедура свеобухватно прописује начин заштите информационо комуникационог система Дома здравља Бор. Свеобухватна заштита подразумева физичко-техничку заштиту ИКТ система од физичких оштећења – влаге, пожара, крађа, недозвољеног приступа, отуђења, уништења и слично, што је у тесној корелацији са Проценом ризика у заштити лица, имовине и пословања.

Информационо комуникациони систем (у даљем тексту ИКТ) Дома здравља Бор, спада у ИКТ систем од посебног значаја . ИКТ системи од посебног значаја су системи чије би угрожавање и прекид функционисања имало озбиљне последице како на саму организацију (Дом здравља Бор) тако и за читаво становништво Града Бора и државу.

На изради Акта о информационој безвбедности Дома здраља Бор учествовали су:

- Директор др Весна Радосављевић
- Правник Југослав Романовић
- Администратор - Оператор ИКТ система Драган Вуловић

I ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система (у даљем тексту: Акт о безбедности), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2. спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
3. подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4. прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
5. свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите

ИКТ СИСТЕМ ДОМА ЗДРАВЉА БОР

- ИКТ систем Дома здравља Бор се састоји од здравственог дела и пословног дела. Основна архитектура ИКТ система се састоји од Клијент-Серверске архитектуре.
- Сви сервери се налазе у сервер соби која је аклиматизована и која је одвојена и заштићена од неовлашћеног приступа садржи 4 сервера, 2 сервера за пословни (апликативни сервер и сервер базе података) и 2 сервера (апликативни сервер и сервер базе података).
- Приступ соби имају администратор ситема и овлашћена лица уз дозволу администратора. У сервер собу се не улази често већ само у крајњој нужди приликом хардверског квара. Софтверски проблеми се решавају помоћу терминал радне станице.
- Приступ серверу је дефинисан корисничким налозима са корисничким именом и лозинком. Кориснички приступи су дефинисани нивом овлашћења које корисник има. Највеће привилегије има Адмнистратор система који даље додељује ниво

приступа операторима система. Сваки приступ и операције над серверима се бележе у лог фаловима којима приступа једино Администратор система.

- Напајње сервера иде преко УПС (беспрекидно напајање електричном енеријом), што омогућује стабилан рад сервера приликом разних прекида напајања електричном енергијом.
- ИКТ служба се налази у посебној просторији. Улаз у просторију је одвојен је вратима која су под камерама и са интерфоном. У оквиру ИКТ просторије се налази сервер соба. Оператор ИКТ система у свом сатаву има има 4 радника која се брину да целокупан информациони сисем функционише без икаквих проблема.

1. Администратор система – Шеф службе
2. Оператера за базе података и коришћење програма
3. Техничар за одржавање ИКТ опреме.

Администратор ИКТ система:

- организује, координира и контролише функционисање информационо комуникационих технологија и послова развија, дефинише и координира припрему ИКТ планова;
- координира израду и припрему ИКТ извештаја;
- доноси одлуке о начину реализације ИКТ послова;
- прати правне прописе и контролише спровођење законитости наменског и економичног трошења ИКТ ресурса;
- контролише наменско коришћење и економичност средстава приликом склапања уговора;
- координира израду општих и појединачних аката у вези са ИКТ пословима и даје мишљење о њима; координира израду ИКТ прегледа и анализа;
- координира пројекте реализације дефинисаних програмских захтева;
- дефинише политике безбедности у информационом систему (ИСО 27001).
- Израђује електронску фактуру

Оператера за базе података и коришћење програма

- помаже корисницима рачунарске инфраструктуре у решавању проблема са коришћењем рачунарске и мрежне опреме – сервера, рачунарских радних станица, мрежне опреме, кабловских и радио веза ;
- помаже корисницима рачунарске инфраструктуре у решавању проблема са коришћењем системског софтвера и сервиса – оперативних система, система за обезбеђивање информационо комуникационих сервиса – електронске поште, интранета, интернета и других;

- помаже корисницима рачунарске инфраструктуре у решавању проблема са коришћењем информационог система, системског софтвера, база података корисника картица, корисничких апликација на картицама и у систему;
- помаже корисницима рачунарске инфраструктуре у решавању проблема са коришћењем система заштите и контроле приступа и коришћења информатичких ресурса и сервиса и изради резервних копија података; води оперативне документације и евиденције.

Техничар за одржавање ИКТ опреме.

- одржава базе података – контрола интегритета, индексирање и израда копија у изабраном клијент – сервер систему за управљање базама података; инсталира, подешава, прати параметре рада, утврђује и отклања узроке поремећаја у раду рачунарске и мрежне опреме – сервера, рачунарских радних станица, мрежне опреме, кабловских и радио веза ;
- инсталира, подешава, прати параметре рада, утврђује и отклања узроке поремећаја у раду системског софтвера и сервиса – оперативних система, система за обезбеђивање информационо комуникационих сервиса – електронске поште, интранета, интернета и других;
- инсталира, подешава, прати параметре рада, утврђује и отклања узроке поремећаја у раду информационог, системског софтвера, база података, корисничких апликација и у систему; инсталира, подешава, прати параметре рада, утврђује и отклања узрока поремећаја у раду система заштите и контроле приступа и коришћења информатичких ресурса и сервиса и израда резервних копија података;
- води оперативну документацију и евиденцију.

Поред горе наведених послова редовно се сваке године чисте радне станице, убацију се лиценца за антивирусни програм и детаљно се скенирају рачунари на вирусе.

- Локална рачунарска мрежа у Дому здравља Бор је 1 гигабитна и пројектована у топологији звезде. За повезивање се користе бакарни каблови са упреденим парицама (УТП) категорије 5Е. Сви комуникациони ормани (мрежна чворишта) су назидни са металним кућиштем и прозирним вратима са бравом. У сваком комуникационом орману се налази дистрибуциони панел са шуко утичницама, печ панел и један или два свича у зависности од броја прикључака. Типови конектора који се користе су РЈ-45.

- Мрежа се састоји од 13 мрежних чворишта, од тога је 11 са 24 прикључака за радне станице и 2 са 16 прикључака за радне станице.
- Сви свичеви су брзине протока 1024 Мбпс(мега бита у секунди) или 1Гбпс (гигабита у секунди)
- Рачунарска мрежа је подељена на три сегмента здравствени, пословни и интернет сегмент. Интернет сигнал се добија оптичким каблом преко посебног рутера , који омогућује да се интернет сигнал селективно пропушта до одређених радних станица које морају да имају излаз на интернет. Такође горе наведени рутер има у себи веома развијени софтвер за администрацију интернет сигнала, те омогућује да радне станице имају селективни приступ само одређеним интернет адресама, што додатно олакшава рад и не оптерећује проток интернет сигнала. Преко интернет сигнала су умрежене и све здравствене амбуланте које се налазе на удаљеним локацијама од Дома здравља Бор. Начин комуникације радне станице у удаљеној амбуланти и сервера у Дому здравља се остварује преко L3VPN прстена (Virtual Private Network) конекције. Брзина Интернет сигнала у Дому здравња Бор је 100/100 Мбпс, док је у удаљеним Амбулантама 10/2 Мбпс
- Физичко веза (локална мрежа у Дому здравља) са крајњим корисником (радна станица) се састоји из три корака:
    1. Веза између активних уређаја (switch)
    2. Веза од активног уређаја (switch) до печ панела (мрежни орман - чвориште)
    3. Веза од печ панела до мрежног прикључка за рачунар
    4. Веза од мрежног прикључка за рачунар до мрежне картице рачунара.
    - Софтвер који се користи у Дому здравља се сатоји из софтвера за здравствени део и софтвер за пословни део ИКТ система.
    - Приступ програму и рад у истом је подељен на три нивоа аутентификације:

        1. Логовање на радну станицу са корисничким налогом дефинисаним у оперативном систему радне станице.
        2. Приступ серверу помоћу РДП конекције где сваки корисник приступа са својим корисничким налогом дефинисаним на серверу.
        3. Логовање у опертивни програм помоћу корисничког налога дефинисаног у самом програму.

    - Пословни део софтвера се користи за све неопходне послове везане за економско правно кадровске потребе Дома здравља Бор. Све фукционалности у програму су максимално аутотоматизоване и олакшавају и убрзавају рад корисника пословног дела програма. Програм за обраду плата успешно комуницира са информационим системом трезора тако да је обрада зараде и уплата исте на ефикасан и брз начин реализована.
    - Здравствени део програма се користи за вођење медицинске евиденције података, вођење елктронског картона пацијената и креирање електронске

фактуре за извршене медицинске услуге Републичком фонду здравственог осигурања РФЗО. У програму се врши аутоматско учитавање шифраника прописаним номенклатурама од стране РФЗО-а. Такође здравствени програм ИКТ система је повезан на Интегрисани здравствени информациони систем Министарства здравља ИЗИС. Сви подаци из електронског картона пацијената се пресликавају на ИЗИС систем, у програму изабрани лекари креирају термине за пријем пацијена, где се термини пресликавају на ИЗИС систем. Лекари упућују пацијенте на специјалистичке прегледе у друге установе кроз програм са терминима а сви подаци се пресликавају на ИЗИС. Комуникација између интерног програма Дома здравља Бор и ИЗИС система и обрнуто је остварена преко сервиса за комуникацију између два информациона система, такође интерни програм комуницира са web сервисом РФЗО-а где се добијају најрелевантнији подаци о статусу осигураног или не осигураног лица. Из здравственог програма се аутоматски генерише број изјава пацијената за изабране лекаре. Програм је повезан на Портал Е_рецепт за прописивање и слање терпије пацијента. Такође здравствени део програма је повезан са ВУЗ (вертикална управљивост у здравству) платформ Министарства здрав РС за размену подтака о пацијенту са свим неопходним захтевима о криптовању и заштити података о личности.

Обавеза примене одредби Акта о безбедности

Члан 3.

Мере заштите ИКТ система које су ближе уређене Актом о безбедности служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за све запослене.

Запослени у ИКТ сектору морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

Драган Вуловић – Систем Администратор – Шеф ИКТ сектора

Лела Јанићијевић - Оператера за базе података и коришћење програма

Јелка Илић - Оператера за базе података и коришћење програма

Небојша Пешић - Техничар за одржавање ИКТ опреме

Предмет заштите

Члан 5.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски

кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре

II МЕРЕ ЗАШТИТЕ

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

Члан 6.

Органи надлежни за спровођење Закона о информационој безбедности су: Министарство трговине, туризма и телекомуникација; Национални ЦЕРТ; Министарство одбране, ЦЕРТ органа власти; ЦЕРТ самосталног оператора ИКТ система; Тело за координацију послова информационе безбедности и посебни ЦЕРТ-ови.

Национални ЦЕРТ је тело које обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу. Национални ЦЕРТ је надлежан да прати инциденте на националном нивоу, да пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима, да реагује по пријављеним или на други начин откривеним инцидентима, тако што пружа савете на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања.

Ово тело такође прати пријављене инциденте на националном нивоу и на основу прикупљених података континуирано израђује анализе ризика и инцидената, подиже свест код грађана, привредних субјеката и органа јавне власти о значају информационе безбедности, води евиденцију Посебних ЦЕРТ-ова, те извештава МТТТ као Надлежни орган на кварталном нивоу о предузетим активностима.

Организациона структура оператора ИКТ система од посебног значаја треба да се рефлектује у ИКТ систему. Прецизније, приступ ИКТ систему од посебног значаја треба да буде условљен радним задужењима и обавезама које свако од запослених има у опису свог радног места, с циљем да се смањи ризик од злоупотреба, неовлашћених приступа, нарушавања интегритета података у ИКТ систему и људске грешке.

Рад запослених у ИКТ систему ДЗ Бор је регулисан следећим инзтерним актима који уређују и обавезе и одговорности у вези са управљањем информационом безбедношћу:

• Правилник о унутрашњој организацији и систематизацији радних места;

• Уговори о раду;

• Изјаве о поверљивости;

• Уговори о чувању поверљивости са правним лицима;

• Правилник о приступу посебно осетљивим подацима и информацијама у ИКТ систему.

Директор доноси појединачни акт, у складу са актом о систематизацији, којим одређује одговорна лица за обезбеђивање и праћење безбедности информационог система Сви запослени морају бити упознати са процедуром заштите безбедности ИКТ система.

Администратор ИКТ система утврђује начин доделе овлашћења за приступ ИКТ систему, степен обуке и квалификацију запослених, начин одобравања приступа запосленима од стране руководиоца, односно непосредно надређеног лица. утврђује се и одговорност сваког запосленог и одговорног лица и прописује дисциплинска одговорност запосленог, у случају непоштовања одредби које уређују информациону безбедност.

Приступ ИКТ систему и рад у истом је подељен на три нивоа аутентификације и дефинисан **Процедуром за поступање са корисничким налогом и лозинком**:

- Логовање на радну станицу са корисничким налогом дефинисаним у оперативном систему радне станице.
- Приступ серверу помоћу РДП конекције где сваки корисник приступа са својим корисничким налогом дефинисаним на серверу.
- Логовање у опертивни програм помоћу корисничког налога дефинисаног у самом програму.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 7

Администратор ИКТ система дозвољава рад на даљину без употребе мобилних уређаја од стране запослених, безбедност рада у случају обављања послова ван просторија Дома здравља Бор, је обезбеђена у удаљеним Амбулантама. ИКТ систем је Дом здравља Бор је повезан са удаљеним Амбулантама преко L3 VPN прстена.

L3 VPN омогућава повезивање удаљених локација Ваше компаније путем креирања виртуелне приватне мреже (VPN) која ради на L3 слоју референтног рачунарског мрежног OSI модела, са брзинама од 128 Кб/с до 100 Мб/с.

Предметно ангажовање и омогућавање обављања задатих и неопходних послова се уређује путем **Процедуре за VPN приступ информационом систему** (у даљем тексту: VPN процедура). VPN процедура дефинише правила и услове за повезивање на мрежу са удаљене локације. Правилном применом утврђеног поступка и начина приступа, на

минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи.

Безбедан начин за рад на даљину је повезивање путем VPN-а (Virtual Private Network-виртуелна приватна мрежа). Реч је о услузи стварања издвојеног тунела између два рачунара на јавној мрежи, који се посебно кодира ради заштите.

Рад на даљину

Радни однос за обављање послова ван просторија послодавца обухвата:

• Рад на даљину;

• Рад од куће;

• Виртуелно радно окружење.

Такође, рад на даљину у смислу овог Акта односи се на ситуацију када је запослени и други радно ангажовани обавезан да изврши одређене послове на мрежи послодавца, а налази се ван просторија послодавца.

Рад на даљину запослених или других радно ангажованих (ангажованих за рад у просторијама послодавца) одобрава Директор преко Правне службе а процедуру реализује и води евиденцију о подацима за пристип Администратор ИКТ ситема.

Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који обављају и у потпуности разумеју своју одговорност

Члан 8

Оператор ИКТ система се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају. Њихове одговорности су утврђене Уговором о раду или о ангажовању за рад ван радног односа и интерним актом.

1. Приликом започињања радног односа:

- Новозапослени се упознаје са интерним актом о безбедности ИКТ система од посебног значаја, потписује изјаву о томе, чиме формално преузима одговорност за поступање са ИКТ системом у складу са интерним актима, односно Законом о информационој безбедности.

- Новозапослени потписује изјаву о поверљивости информација до којих долази у току обављања редовних и ванредних радних активности.

2. У току радног односа:

- Интерни акт о безбедности ИКТ система од посебног значаја мора бити стално доступан свим запосленима на интерном порталу ИКТ система од посебног значаја;

- Једном годишње се организују обуке за запослене који раде у оквиру ИКТ истема од посебног значаја. Суштина ових обука би требало да буде не само у објашњавању правних прописа, већ у анализи конкретних примера кршења закона и лоше праксе. У дефинисаним временским интервалима би такође требало организовати тестирање запослених из области безбедности ИКТ система. Тестирање би, поред чисто теоријских питања, требало да буде засновано на студији случаја из делокруга рада ИКТ система од посебног значаја, где би се од запослених очекивало да одговоре на питање шта би урадили, односно како би поступили у конкретној ситуацији. У случају одговорности запосленог за нарушавање безбедности ИКТ система од посебног значаја, оператор је дужан да покрене одговарајући поступак.

Задужени за обуку коришћења ИКТ система су запослени Оператори ИКТ система.

Оператор ИКТ система у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

• Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;

• Штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама;

• Спроводи програме заштите на конзистентан и уједначен начин у свим организационим јединицама;

• Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

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

Члан 9.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања. Дужности и обавезе које остају важеће и после престанка ангажовања и треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа, односно уговора о ангажовању лица ван радног односа.

Ова мера је ближе одређена:

• Процедуром о правима приступа информационом систему

• Уговором о раду

• Уговором о ангажовању лица ван радног односа

• Споразумом о поверљивости

За поступања приликом престанка запослења или ангажовања задужена је служба за људске ресурсе или надређени руководилац или организациона јединица за информационе технологије, који предузимају 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,

• утврђује начин контакта са бившим запосленим након одласка, • проверава враћене мобилне уређаје и уређаје за преношење података,

• даје налог за укидање налога електронске поште и свих других права приступа систему Оператора ИКТ система 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 < Оператора ИКТ система >

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Оператор ИКТ система је дужан да формира базу информационих добара, опреме и софтвера који се користе за израду, обраду, чување, пренос, брисање и уношење података у оквиру ИКТ система од посебног значаја. База мора да одражава реално стање ИКТ система и да сваки унос у базу буде означен са адекватним нивоом осетљивости и критичности. Такође, за сваки сегмент ИКТ система, уређај, софтвер или податак треба да буде назначена особа која је одговорна за његову безбедност, односно интегритет.

УПРАВА			
РБр	Корисник	Адреса	Оперативни систем
1	Здравствени сервер апп	10.160.64.6	win srv 2019 standard

2	Пословни сервер апп	10.160.64.70	win srv 2019 standard
3	Дата сервер здравствени	10.160.64.60	win srv 2019 standard
4	Дата сервер пословни	10.160.64.50	win srv 2019 standard
5	ВУЗ	10.160.64.61	win 10
6	Мејл	10.160.64.4	win 11 CANNON MULTI
7	Секретарица	10.160.64.5	win 10 EPSON M1200
8	Правник	10.160.64.56	win 11 EPSON M1200
9	Кадрови 1	10.160.64.8	win 11
10	Кадрови 2	10.160.64.9	win 11 EPSON LQ 690
11	Статистика	10.160.64.149	win 7 EPSON M1200
12	Начелник економски	10.160.64.48	win 11 EPSON M1200
13	Суза књига	10.160.64.46	win 11 xerox 3032
14	Весна књига	10.160.64.41	win 11 xerox 3032
15	Јелена књига	10.160.64.44	win 11 EPSON M1200
16	Апотека Немања	10.160.64.57	win 7 EPSON M1200
17	Комерцијала 1	10.160.64.63	win 11 HP MULTI
18	Комерцијала 2	10.160.64.62	win 10 EPSON M1200
19	Обрачунска 1	10.160.64.47	win 11 EPSON M1200
20	Обрачунска 2	10.160.64.59	win 11 EPSON M1200
21	Асигнације	10.160.64.49	win 11 EPSON M1200
22	Фактурно	10.160.64.127	win 7 EPSON M1200
23	ИКТ1	10.160.64.160	win 11 EPSON M1200
24	ИКТ2	10.160.64.161	win 11 EPSON M1200
25	ИКТ3	10.160.64.162	win 11 EPSON M1200
26	ИКТ4	10.160.64.163	win 11 EPSON M1200
27	Архива мејл	10.160.64.10	win 11
28	Снимач разговора из хитне	10.160.64.40	win 7
ОДРАСЛО СТАНОВНИШТВО			
РБр	Корисник	Адреса	Оперативни систем
1	Olp1	10.160.64.69	win10 EPSON LQ690
2	Olp10	10.160.64.73	Win 7 EPSON LQ690
3	OLPO22	10.160.64.104	win11 HP 107A
4	Olp6	10.160.64.106	Win 7 EPSON LQ690
5	InfoOLP	10.160.64.107	Win 7
6	Olp8	10.160.64.108	win10 EPSON LQ690
7	Olp7	10.160.64.109	Win 7
8	Ordinacija7	10.160.64.111	Win 7 EPSON LQ690
9	Olp27	10.160.64.115	Win 7 EPSON LQ690
10	Olp12	10.160.64.122	Win 7 EPSON LQ690
11	Olp14	10.160.64.125	win10
12	Olpinj	10.160.64.135	Win 7
13	Olp15	10.160.64.146	Win 7 EPSON LQ690
14	Olp16	10.160.64.152	win10 EPSON LQ690
15	Olp3	10.160.64.180	win10 EPSON LQ690

16	Olp5	10.160.64.182	win10 EPSON LQ690
17	OLPO31	10.160.64.183	Win 7
18	OLPO30	10.160.64.184	win11 HP 107A
19	OLPO12	10.160.64.185	Win 7
20	OLPO32	10.160.64.186	win11 HP 107A
21	OLPO6	10.160.64.187	win11 HP 107A
22	OLPO24	10.160.64.188	win11 HP 107A
23	OLPO11	10.160.64.189	win11 HP 107A
24	OLPO10	10.160.64.190	win11 HP 107A
25	OLPO23	10.160.64.191	Win 7
26	OLPO17	10.160.64.192	Win 7
27	OLPO18	10.160.64.193	win11 HP 107A
28	Olp37	10.160.64.194	win10 EPSON LQ690
29	OLPO19	10.160.64.195	win11 HP 107A
30	OLPO28	10.160.64.196	Win 7
31	OLPO29	10.160.64.197	win11 HP 107A
32	OLPO34	10.160.64.198	Win 7
33	OLPO35	10.160.64.199	Win 7
34	OLPO8	10.160.64.200	Win 7
35	OLPO5	10.160.64.202	Win 7
36	OLPO13	10.160.64.203	Win 7
37	Olp11	10.160.64.204	win 10 Glavna maca EPSON M1200
38	OLPO9	10.160.64.208	win11 HP 107A
39	OLPO25	10.160.64.251	Win 7
40	OLPO37	10.160.64.252	Win 7
ДЕЧИЈЕ И ШКОЛСКО			
РБр	Корисник	Адреса	Оперативни систем
1	ZDRsaradnik	10.160.64.54	win 10 EPSON M1200
2	Psiholog	10.160.64.55	Win 7
3	DDISPO10 sav mladi	10.160.64.113	win 7 epson m1200
4	DDisp1 salter	10.160.64.118	Win 7
5	SDisp2 salter skolsko	10.160.64.119	Win 7
6	Savetnici skolsko	10.160.64.123	Win 7 EPSON M1200
7	Dsav4	10.160.64.153	Win 7
8	DDISPO6	10.160.64.205	Win 7
9	DDISPO4	10.160.64.206	WIN7 EPSON M1200
10	SDISPO6	10.160.64.207	Win 7
11	SDISPO4	10.160.64.209	Win 7 EPSON LQ690
12	SDISPO5	10.160.64.210	Win 7
13	DDispo1 skolski salter	10.160.64.216	Win 7 EPSON LQ690
14	DDISPO9	10.160.64.217	Win 7
15	DDISPO7	10.160.64.218	Win 7
16	DDisp3 salter decije	10.160.64.220	Win 7
17	DDISPO2	10.160.64.235	Win 7

18	DDISPO5 savetov	10.160.64.237	Win 7
19	DDISPO5A savetov	10.160.64.241	Win 7
20	SDISPO4A sistematski	10.160.64.243	Win 7
21	LOGOPED	10.160.64.232	Win 7 EPSON M1200
22	Glsestra zvorinka	10.160.64.248	Win 7 EPSON M1200
СТОМАТОЛОГИЈА			
РБр	Корисник	Адреса	Оперативни систем
1	STOMO15	10.160.64.71	Win 7
2	STOMO2	10.160.64.72	Win 7
3	STOMO16	10.160.64.226	Win 7
4	STOMO14	10.160.64.227	Win 7
5	STOMO11	10.160.64.228	Win 7
6	STOMO10	10.160.64.229	Win 7
7	STOMO9	10.160.64.230	Win 7
8	STOMO6	10.160.64.231	Win 7
9	STOMO17	10.160.64.255	Win 7
10	Stomatologija1 Šalter	10.160.64.155	Win 7 EPSON M1200
ГИНЕКОЛОГИЈА			
РБр	Корисник	Адреса	Оперативни систем
1	Ginekolog Mira	10.160.64.14	Win 7 EPSON M1200
2	Gina	10.160.64.159	Win 7 EPSON LQ680
3	Gino9	10.160.64.181	Win 7 EPSON M1200
4	GINR3	10.160.64.238	Win 7
5	GINR6	10.160.64.239	Win 7
6	GINR1	10.160.64.240	Win 7
ХИТНА			
РБр	Корисник	Адреса	Оперативни систем
1	HITNAGLTEH	10.160.64.201	WIN 11 EPSON M1200
2	hitnalekari dybhit9	10.160.64.247	Win 7
МЕДИЦИНА РАДА			
РБр	Корисник	Адреса	Оперативни систем
1	MRADA5 lekar	10.160.64.171	Win 7
2	Mrada sestre	10.160.64.172	Win 7 EPSON M1200
ПАТРОНАЖА			
РБр	Корисник	Адреса	Оперативни систем
1	Patron2	10.160.64.12	WIN 11 HP nov EPSON M1200
2	Patron4	10.160.64.76	WIN 11 EPSON M1200
3	dzb (db) Sneza patron	10.160.64.77	WIN10 EPSON M1200 LAPTOP
4	polivalentna - Vesnaja	10.160.64.138	Win 7 EPSON M1200
5	Patron1	10.160.64.144	Win 7
6	Patron3	10.160.64.254	Win 7
7	Patron5	10.160.64.164	Win 7
КУЋНО ЛЕЧЕЊЕ			
РБр	Корисник	Адреса	Оперативни систем

1	KUCNASTA - sestre	10.160.64.145	Win 7
2	KNEGAORD - GLAVNA	10.160.64.214	WIN 11 EPSON M1200

ЕПИДЕМИЛОГИЈА СА ХИГИЈЕНОМ			
РБр	Корисник	Адреса	Оперативни систем
1	HIGIJENA - ZOKI	10.160.64.11	WIN 10 EPSON M1200
2	Epidemiologija	10.160.64.136	win 11 EPSON M1200 + HP MULTI FUNK
3	Higijena -Javorka	10.160.64.156	Win 7 EPSON M1200
4	Medotpad	10.160.64.78	WIN 11 EPSON M1200

СЕРВЕРА	4
КЛИЈЕНТ РАЧУНАРА	120
АМБУЛАНТЕ	29
СПЕЦ АМБУЛАНТЕ	47
УКУПНО КЛИЈЕНТ РАЧУНАРА	196

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

Члан 11.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем за Оператора ИКТ система. Оператора ИКТ система означава типове и локације података као поверљиве, интерне или јавне. ИКТ систем је направио класификациону шему поверљивости информација и базира се на четири нивоа:

• откривање не изазива никакву штету;

• откривање изазива мању непријатност или мању штету;

• откривање има значајан краткорочни утицај на пословање или тактичке циљеве;

• откривање има озбиљан утицај на дугорочне стратешке циљеве или угрожава опстанак.

Оператор ИКТ система > врши класификацију ради:

• Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење;

• Подизања свести о вредности информације или документа;

• Заштите података у покрету ради боље и интелигентније интеграције са DLP, WEB gateway и осталим производима за заштиту параметара и крајњих уређаја;

• Заштите садржаја;

• Интеграције са системима за архивирање.

Оператор ИКТ система поступања у складу са усвојеном Шемом класификовања података. Посебном процедуром се дефинишу радње за поступање, обраду, складиштење и пренос података. #

Процедура о поступању са имовином мора да подразумева:

• ограничења приступа која подржавају захтеве за заштиту сваког нивоа класификације;

• одржавање званичног записа о овлашћеним примаоцима имовине;

• заштиту привремених или трајних копија података на нивоу који је у складу са заштитом оригиналне информације;

• складиштење информационе имовине у складу са спецификацијама произвођача;

• јасно обележавање свих копија медија на које овлашћени прималац треба да обрати пажњу

Све базе података (2 здравствене и 2 пословне) се бекапују сваке ноћи аутоматским подешавањем бекапова. Бекапови се аутоматски копирају на удаљену локацију. Оператор ИКТ система такође чува бекапове база подтака и на екстерном медију.

- Дневни бекапови се чувају 7 дана
- Месечни бекапови се чувају годину дана
- Годињи се чувају трајно

Једном месечно бекапује се и целокупан оперативни систем односно платформа на серверима и ти се бекапови копирају на удаљену локацију. Такође приликом сваког апдејтоиввања нове верзије програма или промене у подешавањима сервер врши се предходно бекаповање база података и бекаповање оперативног система. Бекапови се одмах склањају на удаљену локацију и на екстерни носач података.

Заштита носача података

Члан 12.

Оператор ИКТ система обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података. Евиденцију носача на којима су снимљени подаци, води ИКТ Сектор Дома здравља Бор

Носачи података су све врсте меморијских предмета и уређаја који се користе за складиштење и пренос података. Овај сегмент опреме обухвата дискове који су фиксни део ИКТ система, али и уређаје и носаче који се користе за пренос података, као што су УСБ Фласх меморије, екстерни дискови, ЦД, ДВД и остали предмети и компоненте који имају могућност чувања и преноса података.

Употреба непроверених уређаја и медија представља велики безбедносни ризик који отвара могућност уношења малициозног софтвера у ИКТ системе од посебног значаја.

Управљање преносним носачима података (медијума)

Оператор ИКТ система је дужан да развија и имплементира процедуру о управљању преносним носачима, у складу са усвојеном Шемом класификовања података.

Процедура о управљању преносним носачима може садржати следеће одредбе:

• садржај сваког медијума који се може поново користити и који ће се износити изван организације, онда када више није потребан, треба да се неповратно избрише;

• за све медијуме који се износе из организације, онда када је то неопходно и изводљиво, треба захтевати одобрење, а о свим таквим изношењима треба водити евиденцију, како би се сачувао траг за проверу;

• све медијуме треба складиштити на безбедном и заштићеном месту, у складу са препорукама произвођача;

• коришћење криптографских техника за заштиту података на преносним медијумима, ако су поверљивост или интегритет података важни;

• подаци треба да буду пренети на нови медијум пре него што постану нечитљиви;

• вишеструке копије вредних података треба чувати на одвојеним медијумима да би се додатно смањио ризик од случајног оштећења или губитка података;

• да би се ограничила могућност губљења података, треба предвидети регистровање преносних медијума;

• покретне преносне медијуме треба користити само ако за то постоји пословна потреба;

• уколико постоји пословна потреба за коришћењем преносних медијума, неопходно је пратити пренос података на такве медијуме.

Ограничење приступа подацима и средствима за обраду података

Члан 13

Обављање основне делатности оператора ИКТ система од посебног значаја повезано је са руковањем подацима који се налазе у ИКТ систему. Због тога је неопходно да запосленима буде омогућен приступ различитим подацима у оквиру система. Међутим, приступ запослених овим подацима треба да буде усаглашен са процесном структуром организационог система. Запосленима је потребно обезбедити приступ само оним подацима и деловима ИКТ система који су им потребни за реализацију активности за које су надлежни, а не комплетном ИКТ систему. Стога је потребно прилагодити права приступа ИКТ систему описима послова из важећег правилника о унутрашњој организацији и систематизацији радних места.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности података и усвојеном Шемом класификовања података

према члану 11. овог акта. Оператор ИКТ система формира Контролну листу приступа која садржи попис свих информационих објеката и субјекте који им могу приступити.

Корисницима је дозвољен приступ само мрежи и мрежним услугама за чије коришћење су овлашћени.

#Садржај процедуре о приступу мрежи и мрежним уређајима:

• листа мрежа и мрежних услуга којима је приступ дозвољен;

• начини ауторизације ради утврђивања коме је одобрен приступ, којој мрежи и којим услугама; • начин управљања заштитом приступа мрежним прикључцима и услугама;

• средства која се користе за приступ мрежама и мрежним услугама;

• захтеви у погледу верификације корисника за приступ различитим мрежним услугама;

• начини надгледања коришћења мрежних услуга

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

Члан 14

Оператор ИКТ система управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

Управљање корисничким идентификаторима врши се уз поштовање следећих принципа:

• кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;

• коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење;

• корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;

• периодично идентификовање и уклањање или онемогућавање вишеструких корисничких идентификатора;

• вишеструки идентификатори неког корисника се не издају другим корисницима.

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 одлуке Директора, Правника и Администратора ИКТ система. <

Привилегована права на приступ додељују посебно за сваки системски објекат уз дефинисан рок трајања тих права. 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.

Оператор ИКТ система 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.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15.

Аутентификације корисника којима је одобрен приступ систему врши се путем . 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 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. Администратор ИКТ система има увид у нове шифре.

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

Члан 16.

Заштиту података у ИКТ систему од посебног значаја омогућава енкрипција, односно шифровање података тако да их је немогуће растумачити без шифре. Будући да рачунар све садржаје третира као бројеве, без обзира да ли је реч о тексту или сликама, процес шифровања практично преводи податке у велики скуп бесмислених знакова који се обрнутим процесом, уз помоћ јединственог кључа, враћају у првобитни облик. Коришћење механизама (алгоритама) за енкрипцију мора да буде стандардизовано на нивоу оператора ИКТ система од посебног значаја, те је потребно водити рачуна о крипто кључевима и “хасх” вредностима који се користе за ову врсту заштите.

Оператор мора да пропише адекватне начине генерисања, чувања, дистрибуције, повлачења и брисања крипто кључева. Кључеви се морају чувати у енкриптованој бази са високо рестриктивним приступом, а особа која је задужена за безбедност система и

има висок ниво приступа ИКТ систему, треба да буде овлашћена за њихову администрацију, са посебно високим нивоом одговорности.

Криптозаштита обезбеђује:

• Аутентификацију (идентификацију корисника и других системских ентитета који захтевају приступ или одобрење акције корисника);

• Непорецивост (примена криптографских техника, најчешће дигиталног потписа, како би се добила потврда о извршавању или неизвршавању неке акције од стране појединачног корисника);

• Поверљивост (применом шифровања врши се заштита осетљивих или критичних информација које се складиште или преносе);

• Интегритет (непроменљивост података који се преносе). Поступак криптографске контроле обухвата:

• анализу и процене потреба примене криптографије у пословним процесима укључујући опште принципе према којима би пословне информације требало да се штите;

• ниво заштите се одређује узимањем у обзир типа алгоритма за криптовање података, јачине и квалитета криптографског алгоритма;

• примену шифровања за заштиту осетљивих података приликом преноса мобилним или другим медијумима, уређајима или преко комуникационих водова;

• управљање кључевима (заштита криптографских кључева, повраћај шифрованих података у случају губљења, компромитовања или оштећења кључева).

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

Члан 17.

<Оператор ИКТ система је дужан да предузме мере ради спречавања неовлашћеног физичког приступа < објекту, простору, просторијама, зони >, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација.

Просторије оператора ИКТ система од посебног значаја треба да имају адекватну физичку заштиту у виду алармних система и система за контролу приступа (коришћењем идентификационих картица и сл). Просторије у којима се налазе опрема и документи који су саставни део ИКТ система од посебног значаја треба да буду безбедне зоне у оквиру објекта оператора. Сви сервери треба да буду смештени у посебној сервер сали, у којој се поштују одређене сигурносне мере. Приступ сали мора бити ограничен на службенике из ИТ сектора који су задужени за одржавање система, сервера, мреже и телекомуникација. Такође, сала се мора закључавати сигурносном бравом. На серверима треба да буде јасно означена њихова намена, односно функција и број под

којим су заведени у базу информационих добара. Сервери треба да буду заштићени од свих врста удара и физичких оштећења, од претерано високих или ниских температура, електромагнетних зрачења, као и од сувише високе или ниске влажности ваздуха. Сервери се уобичајено налазе на регалима изнад патоса како би се избегла оштећења у случају поплаве. У сали треба да постоји клима уређај који вентилира ваздух. Такође, веома је важно користити уређаје за непрекидно напајење електричном енергијом (Унинтерруптибле Повер Супплиес - УПС). Сву потребну опрему за безбедност физичког окружења треба редовно одржавати.

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

Члан 18

Постављање и заштита опреме Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа.

#Смернице за безбедност опреме:

• Опрема се поставља на месту које се може обезбедити од неовлашћеног приступа;

• Опрема за обраду информација која служи за приступ и коришћење осетљивих података се поставља не места која нису видљива неовлашћеним особама

• Просторије са опремом треба редовно чистити од прашине;

• Забрањено је конзумирање хране и пића и пушење близини опреме за обраду информација; • Редовно се прате температура и влажност ваздуха;

• Опрема мора бити заштићена од атмосферских падавина;

Оператор ИКТ система редовно прати услове околине, као што су температура и влажност, који би могли негативно да утичу на рад опреме за обраду информација.

Опрема се штити од прекида напајања, тако што се:

• помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;

• капацитет помоћне опреме редовно процењује;

• редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова; • обезбеђује вишеструко напајање са различитих траса.

ИКТ опрема се одржава како би се осигурали њена непрекидна расположивост и неповредивост, и то на следећи начин:

• опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;

• поправке и сервисирање опреме обавља само особље овлашћено за одржавање и Оператор ИКТ система;

• о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;

• пре враћања опреме у рад након одржавања, потребно је прегледати како би проверили да није неовлашћено коришћена или оштећена.

Опрема, информације или софтвер се измештају само уз одобрење одговорног лица, а током измештања се примењују следећа правила:

• треба да се одреде запослени и спољни корисници који имају овлашћење да одобре измештање имовине;

• треба да се поставе временска ограничења за измештање опреме и да се проверава усклађеност приликом повратка;

• треба документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања и ова документација треба да буде враћена са опремом, информацијама или софтвером,

На измештену опрему треба применити безбедносне механизме заштите, узимајући у обзир различите ризике приликом рада изван просторија.

Сви делови опреме који садрже медијуме за чување података потребно је верификовати да би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњени.

Корисници треба да обезбеде да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.

#Процедура:

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. Лаптопови морају бити везани уз помоћ одговарајуће опреме или закључани у фиоци. Таблети и остали преносни уређаји морају бити закључани у фиоци.

5. Носачи података као што су дискови и flash меморија морају бити одложени и закључани.

6. Шифре за приступ не смеју бити написане и остављене на приступачном месту.

7. Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.

8. Материјал који је намењен за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Приступ ИКТ систему треба омогућити само лицима која одржавају систем. Осим овлашћених лица, приступ систему треба обезбедити лицима којима је приступ потребан због појединачног случаја (нпр. на захтев ИКТ система од посебног значаја, приступ вендору произвођачу оперативног програма).

Такође, за приступе с циљем унапређења и развоја ИКТ система, треба направити тестно окружење које је одвојено од оперативног и не садржи осетљиве податке из ИКТ система од посебног значаја. Кориснички приступ систему треба да буде на најнижем нивоу, односно да поседује минималне привилегије и то искључиво делу система који је кориснику потребан за рад.

Такође, систем администатор треба да конфигурише систем тако да се након одређеног времена неактивна сесија прекине. Ово подешавање треба да буде на нивоу целог система, односно да важи за сваког корисника. Софтвер треба ажурирати благовремено и успоставити редовну шему прављења резервних копија. Сваки сервер треба да садржи одређене мере заштите система као што су анти-вирус и заштитни зид (фиревалл). Почетак заштите од злонамерног софтвера је контрола уноса података, софтвера и уређаја у ИКТ систем од посебног значаја.

Управљање расположивим капацитетима

Коришћење ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходнеперформансе система. Периодично се спроводе слеће 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 нисукритичне за пословање.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 20.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Оператору ИКТ сектора

У циљу заштите одупада у ИКТ систем, Оператор ИКТ сектора је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета Оператор ИКТ сектора може укинути приступ.

Заштита од губитка података

Члан 21.

Оператор ИКТ система 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.

DRaaS (Disaster Recovery as a Service)

ДРааС решење поред бекапа омогућава и репликацију целокупног сервера. У року од 6 часова сервер је спреман за рад. Бекап се ради једном недељно или након сваке измене података у оперативном систему на серверу. Бекап се чува на удаљеној локацији и на екстерном носачу података.

Тестирање опоравка система се врши на тестним серверима и на новом серверу риликом подизања оперативног система и након конфигурисања оперативног система.

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

Члан 22.

У ИКТ систему Оператора ИКТ система формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Оператор ИКТ система прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са -информационом безбедношћу, који се морају чувати и редовно преиспитивати. Администратори система немају дозволу да бришу или деактивирају дневнике о сопственим активностима. Записи о догађајима садрже:

• идентификаторе корисника;

• активности система;

• датуме, време и детаље кључних догађаја, нпр. пријављивања и одјављивања;

• идентитет или локацију уређаја, ако је могуће, и идентификатор система;

• записе о успешним и одбијеним покушајима приступа систему;

• записе о успешним и одбијеним покушајима приступа подацима и другим ресурсима;

• промене у конфигурацији система;

• коришћење привилегија;

коришћење системских помоћних функција и апликација;

• датотеке којима се приступало и врсте приступа;

• мрежне адресе и протоколе;

• аларме које је побудио систем за контролу приступа;

• активирање и деактивирање система заштите, као што су антивирусни системи и системи за откривање упада.

#Смернице за контролу промена и инсталацију софтвера:

• ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљени администратори, по добијању одговарајућег овлашћења од руководиоца;

• оперативни системи треба да садрже само одобрене извршне кодове, а не и развојне кодове или компилаторе;

• апликације и оперативни системски софтвер треба имплементирати тек после обимног и успешно спроведеног испитивања, које обухвата испитивање применљивости, безбедности, утицаја на друге системе и погодности за коришћење, а

треба их спроводити на засебним системима, односно тестним окружењима (описано у тачки ... тестирање);

• треба осигурати да су све одговарајуће библиотеке изворних програма ажуриране;

• пре имплементације било каквих промена, треба успоставити стратегију повратка на претходно стање;

• приликом свих ажурирања на библиотекама оперативних програма, треба одржавати записе за проверу;

• као меру предострожности за неочекиване ситуације треба сачувати претходне верзије апликативног софтвера;

• старије верзије софтвера треба архивирати, заједно са свим потребним информацијама и параметрима, процедурама, детаљима конфигурације и софтвером за подршку, све док се подаци држе у архиви.

Инсталацију и подешавање софтвера може да врши само ИКТ Сектор, односно запослени-корисник који има овлашћење за то.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

Оператор ИКТ система врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

Управљање техничким рањивостима Оператор ИКТ система благовремено прикупља информације о техничким рањивостима информационих система који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимањем у обзир припадајућих ризика. Посебне информације које су потребне за подршку управљања техничким рањивостима обухватају продавца софтвера, бројеве верзија, текуће стање размештаја, као и особе које су одговорне за тај софтвер.

#Смернице:

• ИКТ Сектор дефинише и успоставља улоге и одговорности у вези са управљањем техничким рањивостима, укључујући надзор, оцену ризика услед утврђене рањивости, исправке, следљивост имовине и све одговорности за потребна координирања;

• најмање једном месечно, а по потреби и чешће, врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.

• за софтверске и друге технологије засноване на списку имовине: се одређују информациони ресурси за идентификовање одговарајућих техничких рањивости и за

одржавање свести о истима; ови информациони ресурси се ажурирају на основу измена у инвентару или онда када се идентификују нови или други корисни ресурси;

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

Члан 25.

Приликом спровођења ревизије ИКТ система, Оператор ИКТ система обезбеђује да ревизија има што мањи утицај на фукционисање система.

Бекап система и базе података се шаље у тестну лабораторију, произвођача софтвера са којим Дом здравља Бор има склопљен Уговор о испоруци и одржавању софтвера.

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

Члан 27.

Заштита података који се преносе комуникационим средствима унутар < Оператор ИКТ система >, између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

• 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. Другу намену коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника

Безбедан пренос пословних информација између организације и трећег лица обезбеђује се поштовањем споразума о преносу информација.

#Споразуми о преносу информација треба да укључе следеће:

1. одговорности руководства за контролу и извештавање о преносу, отпреми и пријему;

2. процедуре за обезбеђење следљивости и непорецивости;

3. минималне техничке стандарде за паковање и пренос;

4. стандарде за идентификовање курира;

5. обавезе и одговорности у случају инцидената нарушавања безбедности информација, као што је губитак података;

6. коришћење договореног система означавања осетљивих или критичних информација, уз осигуравање да је значење ознака одмах разумљиво и да су те информације заштићене на одговарајући начин;

7. посебне контроле које су потребне да би се заштитили осетљиви детаљи, попут криптографије;

8. одржавање ланца надзора за информације у току преноса.

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

Члан 28.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, < Оператор ИКТ система > је у обавези да обезбеди информациону безбедност у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења.

ИКТ Сектор Дома Здравља Бор је задужен за технички надзор над реализацијом од стране извођача, односно испоручиоца. О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система **ИКТ Сектор Дома Здравља Бор** води документацију. Документација из претходног става мора да садржи описе свих процедура, а посебно процедура које се односе на безбедност ИКТ система.

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

Члан 29.

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера наведених у овом члану. За потребе испитивања и

тестирања ИКТ система, односно делова система, < Оператор ИКТ система > избегава коришћење оперативних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачног добављача, купца, запосленог или др. Уколико се за сврху испитивања користе лични подаци или неке друге поверљиве информације, онда се сви осетљиви подаци и информације пре коришћења штите анонимизацијом личних података, уклањањем садржаја или изменом текста садржаја у предметном делу.

За податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су подаци о личности коришћени приликом тестирања система, одговоран је **ИКТ Сектор Дома Здравља Бор**, у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

За потребе тестирања ИКТ система односно делова система **ИКТ Сектор Дома Здравља Бор** система може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин. Приликом тестирања апликативних система примењују се додатне процедуре за контролу приступа путем физичке заштите и применом криптографских мера за заштиту система и података од неовлашћених приступа, а које се примењују и на оперативним системима. Скуп криптографских мера које ће бити примењене за заштиту података утврђује < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >, узимајући у обзир њихову поузданост исврсисходност.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга Члан 30. Политика безбедности размене информација у пословним односима са пружаоцима услуга и између независних пружалаца услуга Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација

ИКТ Сектор Дома Здравља Бор садржи уговорну одредбу о заштити и чувању поверљивости информација, података и документације. Пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са < Оператор ИКТ система >.

< Оператор ИКТ система > успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга:

• идентификовање и документовање врсте пружаоца услуга којима ће < Оператор ИКТ система > дозволити да приступ информацијама;

• стандардизовани процес за управљање односима између пружаоца услуга;

• дефинисање врста информација које ће различитим типовима пружаоца услуга бити дозвољено ради приступања, праћења и контроле приступа;

• минимални захтеви за безбедност информација за сваку врсту информација и врсту приступа; • процеси и процедуре за праћење придржавања утврђених захтева за безбедност за сваку врсту добављача и врсту приступа;

• контроле за осигурање интегритета информација или обраде информација коју обезбеђује било која страна;

• поступање са инцидентима и непредвиђеним ситуацијама које су у вези са приступом пружаоца услуга, укључујући одговорности и организације и пружаоца услуга;

• управљање неопходним променама информација, опреме за обраду информација и свега осталог што треба да се премешта и осигурање да се безбедност информација одржава током прелазног периода.

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

Члан 32.

Одговорност појединаца и поступак одговора на инциденте Посебним процедурама се уређује начин одговора на инциденте нарушавања информационе безбедности и одређује особа овлашћена за контакт у случајевима нарушавања безбедности, као и контакт санадлежним органима.

#Потребне процедуре

• процедуре за припрему и планирање одговора на инциденте;

• процедуре за надгледање, детекцију, анализу и извештавање о догађајима и инцидентима у вези са безбедношћу информација;

• процедуре за записивање активности у оквиру управљања инцидентима;

• процедуре за поступање са судским доказима;

• процедуре за оцењивање и одлучивање о догађајима у оквиру безбедности информација и оцењивање слабости у погледу безбедности информација;

• процедуре за одговарање на инциденте, опоравак од инцидента и комуникацију са екстерним или интерним особама или организацијама.

Задатак **ИКТ Сектор Дома Здравља Бор**, је да придржавајући се процедура одређених овим чланом, планирају, детектују, анализирају и информишу надлежне у току и након инцидента. **ИКТ Сектор Дома Здравља Бор** подразумева одговарајућа техничка знања како би на најбржи и одговарајућу начин могли да одговоре на безбедносне инциденте. **ИКТ Сектор Дома Здравља Бор** у циљу превенције од безбедносних ризика обезбеђује више (различитих и другачијих) мехнизама за комуникацију и координацију у случају нарушавања безбедности.

Ови еханизми могу бити бити:обезбеђивање контакт информација (број телефона, електронска адреса) појединаца и чланова тима у оквиру организације и ван ње, систем за праћење проблема, шифровани софтвер који би био коришћен од стране појединаца

у оквиру организације и спољашних странака, посебну осигурану просторију за чување података и складиштење поверљивог материјала. У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени- -корисник је дужан да о томе одмах обавести **ИКТ Сектор Дома Здравља Бор**.

Извештавање о догађајима у вези са безбедношћу информација Сви запослени морају бити упознати са обавезом и процедуром извештавања о догађајима у вези са информационом безбедношћу. **ИКТ Сектор Дома Здравља Бор** је у дужан да припреми план и неколико метода комуникације које би могле да се примене у зависности од инцидента.

Могуће методе комуникације су: електорнска пошта, веб сајтови (интерни, екстерни, портали), телефонска комуникација, говорна порука, писмено извештавање, директан контакт.

У случају погрешног функционисања или других аномалијских понашања система врши се исто извештавање као и у случају догађаја у вези са информационом безбедношћу

#Процедура:

1. Запослени који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и послати га електронском поштом сектору за информационе технологије (help desk)/ позвати број/ пријавити проблем путем Интернет стране за help desk;

2. Адресу електронске поште, број телефона и Интернет страну за help desk проверава систем администратор;

3. Систем администратор врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури. Када је индетификован инцидент запослени је дужан да одмах обавести **ИКТ Сектор Дома Здравља Бор**, и предузме мере у циљу заштите ресурса ИКТ система.

ИКТ Сектор Дома Здравља Бор води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Извештавање о утврђеним слабостима система заштите Сви запослени су у обавези да о уоченим и утврђеним слабостима ИКТ система известе **ИКТ Сектор Дома Здравља Бор**, у што краћем року, како би се инциденти нарушавања информационе безбедностиспречили и спречио настанак штете. Одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности, поступа у складу са одговарајућом процедуром.

Догађаји у вези са информационом безбедношћу се оцењују и у складу са анализом се доноси одлука да ли је потребно да се класификују као инциденти нарушавања информационе безбедности.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

Оператор ИКТ система примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

Планирање континуитета мера безбедности информација Континуитет пословања се осигурава кроз План за обезбеђење континуитета пословања и План опоравка од нежељених догађаја ИКТ система.

#При изради Плана за обезбеђење континуитета пословања за хардверске компоненте ИКТ система треба обухватити следеће:

- документацију за логички и физички дијаграм и копије пројеката;

- заштитне копије конфигурационих фајлова и оперативног система активних уређаја;

- постојање резервне опреме;

- унапред направљене конфигурације за различите сценарије;

- израду резервних копија.

#При изради Плана опоравка од нежељених догађаја ИКТ система:

- проценити најкритичније апликације, податке, конфигурационе фајлове и системски софтвер за који треба направити резервне копије;

- одредити место чувања копије;

- одредити нову локацији рада ИКТ система у случају немогућности рада на основној локацији/избор рачунара који ће привремено заменити сервер док се сервер не стави у функцију.;

- навести податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја;

- одредити изворе непрекидног напајања електричном енергијом.

Такође, при изради Плана опоравка од нежељених догађаја ИКТ система потребно је предвидети:

- постојање документације за сервисе, апликације и базе података;

- процедуре инсталације и конфигурисања сервиса, апликација и база података;

- место чувања инсталација сервиса, апликација и база података и резервне копије података;

- податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја;

- развијене и одобрене документоване планове, одговоре и процедуре за опоравак, детаљно наводећи како ће организација управљати догађајима који узрокују поремећаје и како ће одржавати своју безбедност информација.

Имплементација континуитета безбедности информација Да би се осигурао потребан ниво континуитета безбедности информација током ванредних ситуација, **ИКТ Сектор Дома Здравља Бор** примењује процедуре и контроле описане у Плану за обезбеђење континуитета пословања.

ИКТ Сектор Дома Здравља Бор редовно врши проверу усвојених процедура контроле континуитета безбедности информација, како би оне биле адекватне и ефективне током ванредних ситуација. Провера се врши вежбањем и испитивањем знања и рутине приликом руковања процесима, процедурама и контролама, као и преиспитивањем ефективности мера безбедности информација у случају промене информационих система, процеса, процедуре и контроле безбедности информација.

III ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Оператора ИКТ система

Члан 34.

Обавеза Оператора ИКТ система је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Оператора ИКТ система.

Ступање на снагу Акта о безбедности

Члан 35.

Овај Акт о безбедности ступа на снагу даном доношења.

УПРАВНИ ОДБОР

БРОЈ:443/4

ДАНА: 29.01.2024. год