Република Србија
Аутономна покрајина Војводина
Покрајински секретаријат за
здравство
Булевар Михајла Пупина 16, 21000 Нови Сад
Т: +381 21 487 4385 Ф: +381 21 456 119
psz@vojvodina.gov.rs

Број: 001355151 2024 80253 001 000 000 001 Датум: 12.4.2024. године

На основу члана 8. став 1. 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) и члана 16. став 1. и 24. став 2. Покрајинске скупштинске одлуке о покрајинској управи („Службени лист АПВ”, број 37/14, 54/14-др. одлука и 37/16, 29/17, 24/19, 66/20 и 38/21), Покрајински секретар за задравство доноси

Правилник о безбедности информационо-комуникационог система Покрајинског секретаријата за здравство

I ОСНОВНЕ ОДРЕДБЕ

Значење појединих термина

Члан 1.

Поједини термини у овом правилнику имају следеће значење:

1) информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата:

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

2) оператор ИКТ система је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3) информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет,

расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

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

5) интегритет значи очуваност изворног садржаја и комплетности податка;

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

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

8) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

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

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

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

11а) јединствени систем за пријем обавештења о инцидентима је информациони систем у који се уносе подаци о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности;

12) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

13) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

20) криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

24) информациона добра обухватају програмски кôд, конфигурацију хардверских компонената, техничку документацију (корисничка упутства, уговори о одржавању опреме и др.), корисничку документацију (документа која креирају и користе запослени током обављања послова), записе о коришћењу хардверских компоненти, податаке из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично.

Предмет уређивања

Члан 2.

Овим правилником 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 информационо-комуникационог система Покрајинског секретаријата за здравство (у даљем тексту: ИКТ систем).

Оператори ИКТ система

Члан 3.

Покрајински секретаријат за здравство и Управа за заједничке послове покрајинских органа су оператори ИКТ система.

Циљеви овог правилника

Члан 4.

Циљеви доношења овог правилника 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.

Обавеза примене одредби правилника

Члан 5.

Мере заштите ИКТ система су ближе уређене овим правилником и служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за јавне функционере, службенике на положају, запослене и на други начин радно ангажована лица у Покрајинском секретаријату за здравство (у даљем тексту: запослени).

Руководиоци организационих јединица у Покрајинском секретаријату за здравство одговорни су за праћење примене мера безбедности у организационим јединицама којима руководе, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност лица

Члан 6.

Одговорност запослених у вези са питањима од значаја за безбедност информационо-комуникационог система су регулисана Упутством о употреби рачунара у мрежном окружењу ("Службени лист АПВ", број: 09-3/2014 од 09.07.2014. године) Покрајинске владе (у даљем тексту: Упутства о употреби рачунара).

Предмет заштите

Члан 7.

Мере заштите ИКТ система односе се на:

(1) електронске комуникационе мреже,
(2) електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма,
(3) оперативне и апликативне рачунарске програме,
(4) податке који се воде, чувају, обрађују, претражују или преносе помоћу мреже или уређаја, а у сврху рада, употребе, заштите или одржавања наведене мреже и уређаја, као што су: кориснички налози, тајне информације за проверу веродостојности (шифре, лозинке), корисничка документација - документа која креирају и користе запослени током обављања послова (подаци у датотекама и базама података, техничка документација (корисничка упутства, уговори о одржавању опреме и др), програмски кôд, записи о коришћењу хардверских компоненти и друго и
(5) организациону структуру путем које се управља ИКТ системом а чији рад је уређен унутрашњим општим актима и процедурама.

II МЕРЕ ЗАШТИТЕ

1. МЕРА - УСПОСТАВЉАЊЕ ОРГАНИЗАЦИОНЕ СТРУКТУРЕ, СА УТВРЂЕНИМ ПОСЛОВИМА И ОДГОВОРНОСТИМА ЗАПОСЛЕНИХ, КОЈОМ СЕ ОСТВАРУЈЕ УПРАВЉАЊЕ ИНФОРМАЦИОНОМ БЕЗБЕДНОШЋУ

Члан 8.

Послови, одговорности и обавезе запослених који се поред осталог односе и на управљање информационом безбедношћу уређују се интерним актима која доноси покрајински секретар, као и општим актима која доноси Покрајинска влада или други надлежни покрајински орган којима се

уређују обавезе и одговорности на нивоу органа Аутономне покрајине Војводине, покрајинских посебних управних организација, секретаријата Покрајинске владе, служби, управа и дирекција.

Покрајински секретаријат за здравство води евиденцију аката од значаја за информациону безбедност сходно 12. члану овог правилника.

2. МЕРА - ПОСТИЗАЊЕ БЕЗБЕДНОСТИ РАДА НА ДАЉИНУ И УПОТРЕБЕ МОБИЛНИХ УРЕЂАЈА

Члан 9.

Покрајински секретаријат за здравство дозвољава рад на даљину и употребу мобилних уређаја од стране запослених, уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја.

Рад на даљину

Радни однос за обављање послова ван просторија послодавца обухвата: рад на даљину, рад од куће и виртуелно радно окружење.

Рад на даљину односи се и на ситуацију када је запослени обавезан да изврши одређене послове на мрежи послодавца, а налази се ван просторија послодавца.

Захтев за удаљени приступ за запосленог који локални администратор у смислу члана 2. став 2. Упутства о употреби рачунара (у даљем тексту: локални администратор) доставља Управи за заједничке послове покрајинских органа претходно одобрава руководилац организационе јединице или подсекретар у Покрајинском секретаријату за здравство.

Коришћење мобилних уређаја

Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Употреба и коришћење уређаја из става 1. овог члана који су у јавној својини Аутономне покрајине Војводине уређена је општим актима надлежног покрајинског органа.

3. МЕРА - ОБЕЗБЕЂИВАЊЕ ДА ЛИЦА КОЈА КОРИСТЕ ИКТ СИСТЕМ, ОДНОСНО УПРАВЉАЈУ ИКТ СИСТЕМОМ, БУДУ ОСПОСОБЉЕНА ЗА ПОСАО КОЈИ ОБАВЉАЈУ И У ПОТПУНОСТИ РАЗУМЕЈУ СВОЈУ ОДГОВОРНОСТ

Члан 10.

Покрајински секретаријат за здравство се стара о спровођењу провере испуњености услова кандидата за запослење и о стручном усавршавању запослених чиме се обезбеђује да запослени који учествују у управљању ИКТ системом и запослени који користе ИКТ систем имају у вези са информационом безбедношћу адекватан степен образовања и оспособљености за обављање послова радног места на које се распоређују.

Сви запослени којима је додељен приступ поверљивим информацијама, морају потписати Изјаву о заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Запослених су дужни да приликом обављањем послова радног места на које су распоређени воде рачуна о безбедност ИКТ система, односно о безбедности информација.

Запослени су у обавези да у склопу реализације планова стручног усавршавања запослених у Покрајинском секретаријату за здравство прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања у вези са информационом безбедношћу, на начин који одговара њиховом пословном ангажовању и радном месту.

4. МЕРА - ЗАШТИТА ОД РИЗИКА КОЈИ НАСТАЈУ ПРИ ПРОМЕНАМА ПОСЛОВА ИЛИ ПРЕСТАНКА РАДНОГ АНГАЖОВАЊА ЗАПОСЛЕНИХ ЛИЦА

Члан 11.

Запослени су дужни да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система и након престанка или промене радног ангажовања.

За поступања са информационим добрима приликом престанка запослења или радног ангажовања покрајински секретар доноси посебну процедуру.

5. МЕРА - ИДЕНТИФИКОВАЊЕ ИНФОРМАЦИОНИХ ДОБАРА И ОДРЕЂИВАЊЕ ОДГОВОРНОСТИ ЗА ЊИХОВУ ЗАШТИТУ

Члан 12.

Оператори ИКТ система из члана 3. овог правилника врше идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информација обухвата креирање, обраду, складиштење, пренос и брисање и уништавање податакаи информација.

Покрајински секретаријат за здравство врши идентификацију и попис информационих добара ИКТ система, односно води Евиденцију информационих добара ИКТ система, која обухвата: (а) Евиденцију средстава за обраду података ИКТ система која су у власништву наведеног секретаријата, (б) Евиденцију рачунарских програма/апликативних софтвера које користе запослени у наведеном секретаријату и (в) Евиденцију аката и процедура од значаја за информациону безбедност ИКТ система.

Евиденција информационих добара ИКТ система из става 1. овог члана се једном годишње ажурира.

Попис, односно евиденција из става 1. овог члана не односи се на информациона добара чија је заштита у целости у надежности и у власништву Управе за заједничке послове покрајинских органа (персонални рачунари, преносни рачунари, уређаји за копирање и скенирање са ИП адресом, телефони са ИП адресом, мобилни телефони, мрежа, сервер, датотеке и базе података, програмски кôд, конфигурација хардверских компоненти, записи о коришћењу хардверских компоненти, техничка и корисничка документација и др.)

Евиденцију средстава за обраду података ИКТ система која су у власништву Покрајинског секретаријата за здравство из става 1. овог члана води локални администратор и иста садржи следеће податке: инвентарне бројеве средстава за обраду података која су у власништву Покрајинског секретаријата за здравство, имена запослених који их користе, годину набавке и друге податке релевантне за спровођење мера заштите предвиђених Законом о информационој безбедности.

Евиденцију рачунарских програма/апликативних софтвера ИКТ система из става 1. овог члана води лице које одреди покрајински секретар и иста садржи следеће податке:

-назив рачунарског програма/апликативног софтвера (даље: софвер);

-назив власника софтвера, а за софтвере чији је власник Покрајински секретаријат за здравство наведена евиденција такође садржи и податак о години куповине и друге релевантне податке из уговора о куповини софтвера, основне податке о одржавању софтвера (да ли је уговорено оржавање софтвера, на који период, подаци о пружаоцу услуге одржавања, контакт подаци и др);

-врста података који се обрађују софтвером и који чине корисничку документацију;

-имена запослених који имају приступ софтверу, односно КОНТРОЛНУ ЛИСТУ ПРИСТУПА у смислу 15. члана овог правилника;

-КЛАСИФИКАЦИЈУ ПОВЕРЉИВОСТИ ПОДАТАКА који се обрађују софтвером, односно информацију о нивоу осетљивости наведених података у смислу члана 13. овог правилника и

-друге податке релевантне за спровођење мера заштите предвиђених Законом о информационој безбедности.

Евиденцију о информационим добрима у смислу општих аката и процедуре од значаја за информациону безбедност ИКТ система из става 1. овог члана води лице које одреди покрајински секретар.

6 МЕРА - КЛАСИФИКОВАЊЕ ПОДАТАКА ТАКО ДА НИВО ЊИХОВЕ ЗАШТИТЕ ОДГОВАРА ЗНАЧАЈУ ПОДАТАКА У СКЛАДУ СА НАЧЕЛОМ УПРАВЉАЊА РИЗИКОМ ИЗ ЧЛАНА 3. ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

Члан 13.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем за примену начела управљања ризиком у Покрајински секретаријат за здравство.

Покрајински секретаријат за здравство означава типове података као поверљиве, интерне или јавне и одређује њихове локације по именима запослених који имају право на приступ тим подацима. Наведени подаци о локацији података се воде како би се у сарадњи са Управом за заједничке послове покрајинских органа, која води евиденцију инвентарних бројева, ИП адреса средстава за обраду података и имена запослених који користе поједина средства за обраду података, могло обезбедити спровођење мера за заштиту информационе безбедности и реаговање на безбедносне ризике и инциденте.

Покрајински секретаријат за здравство доноси Шему класификовања података на четири нивоа:

- откривање података и информација не изазива никакву штету;
- откривање података и информација изазива мању непријатност или мању штету;
- откривање података и информација има значајан краткорочни утицај на пословање или тактичке циљеве;
- откривање података и информација има озбиљан утицај на дугорочне стратешке циљеве или угрожава опстанак.

Покрајински секретаријат за здравство врши класификацију ради:

- јачања одговорности запослених, како би они као корисници ИКТ система могли да уоче и препознају пословну вредност податка приликом чувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење података;
- подизања свести о вредности информације или документа;
- заштите садржаја информација и др.

7. МЕРА - ЗАШТИТА НОСАЧА ПОДАТАКА

Члан 14.

Оператори ИКТ система у смислу члана 3. овог правилника обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података.

Евиденција носача података ИКТ система се води на начин утврђен чланом 12. овог правилника.

Управљање преносним носачима података

Правилник о коришћењу преносних меморија, који доноси покрајински секретар, ближе уређује управљање преносним носачима података, усклађује се са Шемом класификовања података из члана 13. овог правилника.

Расходовање носача података

Када више нису потребни, носачи података се расходују на безбедан начин, односно на начин којим се ризик од могућег преузимања осетљивих података и лиценцираних софвера од стране неовлашћених особа своди на минимум.

Покрајински секретар доноси Процедуру за безбедно расходовање носача података.

Физички пренос носача података

Носачи података који садрже информације штите се од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта.

Физички пренос носача података ближе је уређен Упутством о начину селидбе и премештаја запослених у покрајинским органима, број: 109-031-150/2012 од 3.12.2012. године Управе за заједничке послове покрајинских органа.

8. МЕРА - ОГРАНИЧЕЊЕ ПРИСТУПА ПОДАЦИМА И СРЕДСТВИМА ЗА ОБРАДУ ПОДАТАКА

Члан 15.

Подацима и средствима за обраду података је ограничен приступ у складу са утврђеним степеном тајности података и усвојеном Шемом класификовања података према члану 13. овог правилника.

Покрајински секретаријат за здравство води Контролну листу приступа, односно евиденцију која садржи попис запослених који могу приступити појединим подацима класификованим према степену поверљивости, као и одговарајућим средствима за обраду наведених података.

Запосленима је дозвољен приступ само мрежи и мрежним услугама за чије коришћење су овлашћени што је регулисано Упутством о употреби рачунара.

9. МЕРА - ОДОБРАВАЊЕ ОВЛАШЋЕНОГ ПРИСТУПА И СПРЕЧАВАЊЕ НЕОВЛАШЋЕНОГ ПРИСТУПА ИКТ СИСТЕМУ И УСЛУГАМА КОЈЕ ИКТ СИСТЕМ ПРУЖА

Члан 16.

Мера: Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа је регулисана Упутством о употреби рачунара.

10. МЕРА - УТВРЂИВАЊЕ ОДГОВОРНОСТИ КОРИСНИКА ЗА ЗАШТИТУ СОПСТВЕНИХ СРЕДСТАВА ЗА АУТЕНТИФИКАЦИЈУ

Члан 17.

Мера: Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију је регулисана Упутством о употреби рачунара.

11. МЕРА - ПРЕДВИЂАЊЕ ОДГОВАРАЈУЋЕ УПОТРЕБЕ КРИПТОЗАШТИТЕ РАДИ ЗАШТИТЕ ТАЈНОСТИ, АУТЕНТИЧНОСТИ ОДНОСНО ИНТЕГРИТЕТА

Члан 18.

Мера: Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета је у надлежности Управе за заједничке послове покрајинских органа сходно члановима 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

12. МЕРА - ФИЗИЧКА ЗАШТИТА ОБЈЕКАТА, ПРОСТОРА, ПРОСТОРИЈА ОДНОСНО ЗОНА У КОЈИМА СЕ НАЛАЗЕ СРЕДСТВА И ДОКУМЕНТИ ИКТ СИСТЕМА И ОБРАЂУЈУ ПОДАЦИ У ИКТ СИСТЕМУ, КОНТРОЛА ФИЗИЧКОГ УЛАСКА У ОБЈЕКАТ, ЗАШТИТА КАНЦЕЛАРИЈА, ПРОСТОРИЈА, СРЕДСТАВА, КАО И ЗАШТИТА ОД ПРЕТЊИ ЕКСТЕРНИХ ФАКТОРА ИЗ ОКРУЖЕЊА

Члан 19.

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

заштита канцеларија, просторија, средстава, као и заштита од претњи екстерних фактора из окружења је у надлежности Управе за заједничке послове покрајинских органа, што је регулисано члановима 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа, као и Упутством о унутрашњем реду у згради владе Аутономне Покрајине Војводине и коришћењу паркинг простора ("Службени лист Аутономне Покрајине Војводине", број 031-176/2011 од 6.12.2011. године).

Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у наведеном систему, контрола физичког уласка у објекте, заштита канцеларија, просторија, средстава, као и заштита од претњи екстерних фактора из окружења у објектима у којима су пословне просторије одељења и одсека санитарне инспекције је уређена актима којима се регулишу питања безбедности наведених објеката од стране носилаца права коришћења тих објеката - локаних самоуправа.

13. МЕРА - ЗАШТИТА ОД ГУБИТКА, ОШТЕЋЕЊА, КРАЂЕ ИЛИ ДРУГОГ ОБЛИКА УГРОЖАВАЊА БЕЗБЕДНОСТИ СРЕДСТАВА КОЈА ЧИНЕ ИКТ СИСТЕМ

Члан 20.

Мера: Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем је у надлежности Управе за заједничке послове покрајинских органа, што је регулисано чланом 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа, а у објектима у којима су пословне просторије одељења и одсека санитарне инспекције је уређена актима којима се регулишу питања безбедности наведених објеката од стране носилаца права коришћења тих објеката - локаних самоуправа.

Запослени су дужни да код опреме коју користе и која садржи носаче података, а која је враћена у рад након одржавања, провере комплетност осетљивих информација које су у њој похрањене.

Измештање и премештање имовине

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

- Покрајински секретар овлашћује руководиоце задуженог за одобравање измештања имовине;
- Овлашћени руководилац треба да: поставе временска ограничења за измештање опреме, информација или софтвера и да проверава усклађеност приликом повратка, да одреди начин документовања идентитета и улоге лица која користе или поступају са имовином приликом премештања, а ова документација треба да буде враћена са опремом, информацијама или софтвером.

Безбедност измештене опреме и имовине

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

Безбедност опреме без надзора

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

Остављање осетљивих и поверљивих докумената и материјала

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.

14. МЕРА - ОБЕЗБЕЂИВАЊЕ ИСПРАВНОГ И БЕЗБЕДНОГ ФУНКЦИОНИСАЊА СРЕДСТАВА ЗА ОБРАДУ ПОДАТАКА

Члан 21.

Мера: Обезбеђивање исправног и безбедног функционисања средстава за обраду података је регулисана Упутством о употреби рачунара.

Усвајање и примена радних процедура, смерница и инструкција

Покрајински секретар за здравство доноси смернице, процедуре и инструкције које се односе на функционисање ИКТ система у погледу: обраде и поступања са информацијама, израде резервних копија и управљања поверљивим подацима.

Остале смернице, процедуре и инструкције су у надлежносту Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

15. МЕРА - ЗАШТИТА ПОДАТАКА И СРЕДСТАВА ЗА ОБРАДУ ПОДАТАКА ОД ЗЛОНАМЕРНОГ СОФТВЕРА

Члан 22.

Мера: Заштита података и средстава за обраду података од злонамерног софтвера је у надлежносту Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

Поступак контроле и предузимање мера против злонамерног софтвера

Поступци контроле и предузимање мера против злонамерног софтвера су регулисани Упутством о употреби рачунара.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета одлуком одоворног лица може се укинути или ограничити приступ Интернету.

16. МЕРА - ЗАШТИТА ОД ГУБИТКА ПОДАТАКА

Члан 23.

Мера: Заштита од губитка података је у надлежносту Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

Начин организовања заштите од губитка података и обавезе запослених у вези са овим су регулисани Упутством о употреби рачунара.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Покрајиснки секретаријат за здравство доноси План израде резервних копија за податке које процењује као осетљиве и критичне и за које је потребно правити резервне копије и води евиденцију урађених резервних копија.

17. МЕРА - ЧУВАЊЕ ПОДАТАКА О ДОГАЂАЈИМА КОЈИ МОГУ БИТИ ОД ЗНАЧАЈА ЗА БЕЗБЕДНОСТ ИКТ СИСТЕМА

ЧЛАН 24.

Мера: Чување података о догађајима који могу бити од значаја за безбедност ИКТ система (израда записа о догађајима, односно логова и бележење активности корисника, затим записи о активности администратора и оператора система, као и заштита информација у записима) је у надлежности Ураве за заједничке послове покрајинских органа, у складу са чланом 1. и 2. чланом Одлуке о Управи за заједничке послове покрајинских органа.

18. МЕРА - ОБЕЗБЕЂИВАЊЕ ИНТЕГРИТЕТА СОФТВЕРА И ОПЕРАТИВНИХ СИСТЕМА

Члан 25.

Мера: Обезбеђивање интегритета софтвера и оперативних система је у надлежности Управе за заједничке послове покрајинских органа, у складу са чланом 1. и 2. чланом Одлуке о Управи за заједничке послове покрајинских органа, а начин спровођења мере је регулисан Упутством о употреби рачунара.

19. МЕРА - ЗАШТИТА ОД ЗЛОУПОТРЕБЕ ТЕХНИЧКИХ БЕЗБЕДНОСНИХ СЛАБОСТИ ИКТ СИСТЕМА

Члан 26.

Мера: Заштита од злоупотребе техничких безбедносних слабости ИКТ система је у надлежности Управе за заједничке послове покрајинских органа, у складу са чланом 1. и 2. чланом Одлуке о Управи за заједничке послове покрајинских органа, а начин спровођења мере је регулисан Упутством о употреби рачунара.

20. МЕРА - ОБЕЗБЕЂИВАЊЕ ДА АКТИВНОСТИ НА РЕВИЗИЈИ ИКТ СИСТЕМА ИМАЈУ ШТО МАЊИ УТИЦАЈ НА ФУНКЦИОНИСАЊЕ СИСТЕМА

Члан 27.

Мера: Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система, односно планирање и спровођење ревизије ИКТ система је у надлежности Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

21. МЕРА - ЗАШТИТА ПОДАТАКА У КОМУНИКАЦИОНИМ МРЕЖАМА УКЉУЧУЈУЋИ УРЕЂАЈЕ И ВОДОВЕ

Члан 28.

Мера: Заштита података у комуникационим мрежама укључујући уређаје и водове је у надлежности Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

22. МЕРА - БЕЗБЕДНОСТ ПОДАТАКА КОЈИ СЕ ПРЕНОСЕ УНУТАР ПОКРАЈИНСКОГ СЕКРЕТАРИЈАТА ЗА ЗДРАВСТВО, КАО И ИЗМЕЂУ ПОКРАЈИНСКОГ СЕКРЕТАРИЈАТА ЗА ЗДРАВСТВО И ТРЕЋЕГ ЛИЦА

Члан 29.

Заштита података који се преносе комуникационим средствима унутар Покрајинског секретаријата за здравство, као и између Покрајинског секретаријата за здравство и трећег лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

Правила коришћења електронске поште, правила коришћења Интернета и размене електронских порука и правила коришћења информационих ресурса су регулисана Упутством о употреби рачунара и овим правилником.

Споразуми о преносу информација

Безбедан пренос пословних информација између Покрајинског секретаријата за здравство и трећег лица може бити регулисан склапањем споразума о преносу информација.

Споразуми о поверљивости или неоткривању

Заштита информација Покрајинског секретаријата за здравство и обавезивање потписника да информације штите, користе и објављују на одговоран и ауторизован начин може бити регулисана споразумом о поверљивости или неоткривању.

23. МЕРА - ИСПУЊАВАЊЕ ЗАХТЕВА ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ У ОКВИРУ УПРАВЉАЊА СВИМ ФАЗАМА ЖИВОТНОГ ЦИКЛУСА ИКТ СИСТЕМА ОДНОСНО ДЕЛОВА СИСТЕМА

Члан 30.

Мера: Испуњавање захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система (фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе ИКТ система) је у надлежности Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

Обезбеђивање апликативних услуга у јавним мрежама

Информације обухваћене апликативним услугама које пролазе кроз јавне мреже треба заштити од малверзација, неовлашћеног откривања података и модификовања. Неопходно је утврдити идентитет корисника и извршити поделу овлашћења и одговорнности за постављање садржаја, електронског потписивања или обављања трансакција, о чему Покрајински секретаријат за здравство сходно члану 12., 13. и 15. овог правилника води евиденцију, класификује податке и утврђује Контролну листу приступа.

24. МЕРА - ЗАШТИТА ПОДАТАКА КОЈИ СЕ КОРИСТЕ ЗА ПОТРЕБЕ ТЕСТИРАЊА ИКТ СИСТЕМА ОДНОСНО ДЕЛОВА СИСТЕМА

Члан 31.

Мера: Заштита података који се користе за потребе тестирања ИКТ система односно делова система је у надлежности Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

25. МЕРА - ЗАШТИТА СРЕДСТАВА ЗА ОБРАДУ ПОДАТАКА ОПЕРАТОРА ИКТ СИСТЕМА КОЈА СУ ДОСТУПНА ПРУЖАОЦИМА УСЛУГА

Члан 32.

Мера: Заштита средстава за обаду података оператора ИКТ система која су доступна пружаоцима услуга је у надлежности Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа, а у изузетним случајевима и у складу са планским актима и активностима, када Покрајински секретаријат за здравство кроз спроведени одговарајући поступак ангажује пружаоца услуга којем је потребно омогућити приступ деловима ИКТ система, постоји и надлежност наведеног секретаријата.

Политика безбедности размене информација у пословним односима Покрајинског секретаријата за здравство са пружаоцима услуга и између независних пружалаца услуга

Покрајински секретаријат за здравство, на основу претходно одобреног захтева за инсталирањем одређеног софтвера у ИКТ систему на начин утврђен чланом 26. Упутства о употреби рачунара, успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга на следеће начине:

- управљање односима са пружаоцима услуга којима је ради извршења уговорних обавеза потребно омогућити приступ ИКТ систему регулише се закљученим уговором;

- сходно члану 12. овог правилника Покрајински секретаријат за здравство води евиденцију која садржи податке о софтверима, о врстама и нивоу поверљивости података који се обрађују појединим софтверима, као и податке о и правним и физичким лицима којима је на основу уговора омогућен приступ наведеним софтверима и подацима.

Уговори које Покрајински секретаријат за здравство закључује са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација ИКТ система морају

садржати 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.

Уговори које Покрајински секретаријат за здравство закључује са пружаоцима услуга такође треба да садрже:

- одредбу о праћењу извршења услуга, укључујући праћење придржавања утврђених захтева који се односе на безбедност и осигурање интегритета информација, која садржи и одређивање администратора информационог система, односно лица из члана 2. Упутства о употреби рачунара и/или других запослених који су задужних за праћење извршења услуге у име Покрајинског секретаријата за здравство.

- поступање са инцидентима и непредвиђеним ситуацијама које су у вези са приступом пружаоца услуга, укључујући одговорности и оператора ИКТ система 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.

Уговарање обавезе обезбеђивања безбедности у споразумима са пружаоцима услуга

Пре закључења уговора потенцијални пружалац услуга у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, која садржи обавезу за пружаоца услуга да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране оператора ИКТ система у смислу члана 3. овог правилника, а за потребе извршења предмета будућег уговора.

Потребно је да изјава о поверљивости, односно уговор о пружању услуга, садржи одредбу о поверљивости са јасно утврђеном обавезом и одговорношћу пружаоца услуге уз претњу раскида уговора и накнаде штете у корист оператора ИКТ система у смислу члана 3. овог правилника у случају повреде ове одредбе.

Пружаоци услуга дужни су да захтеве оператора ИКТ система у смислу члана 3. овог правилника у погледу безбедности информација прошире и на евентуалне подизвођаче или остале учеснике у заједничкој понуди за додатне услуге или производе.

26. МЕРА - ОДРЖАВАЊЕ УГОВОРЕНОГ НИВОА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ И ПРУЖЕНИХ УСЛУГА У СКЛАДУ СА УСЛОВИМА КОЈИ СУ УГОВОРЕНИ СА ПРУЖАОЦЕМ УСЛУГА

Члан 33.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга, у складу са условима које је Покрајински секретаријат за здравство уговорио са пружаоцем услуга, лица из 5. става 32. члана овог правилника сачињавају и спроводе План мера надзора и заштите за време пружања услуга и након извршеног посла.

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга

Планом мера надзора и заштите за време пружања услуга и након извршеног посла обезбеђује се редовно праћење, анализа, преиспитивање и провера извршене услуге и усаглашеност са одредбама уговора, на следећи начин:

1. Надгледање и преиспитивање услуга се може вршити преко трећег лица;
2. Неопходно је да се поштују сви услови из споразума или уговора у вези са безбедношћу информација, као и да се спрече сви инциденти и проблеми нарушавања безбедности, те омогући управљање на одговарајући начин;
3. Врши се оцена квалитета извршења и саобразности уговорене услуге;

4. Обезбеђује се контрола над спровођењем услуга и осигурава увид у све осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа страна приступа, које процесуира или којима управља;

5. Обезбеђује се увид у безбедносне активности кроз јасно дефинисан процес извештавања.

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене, утврдити поступак извештавања, праћења и поступања у складу са захтевима Покрајинског секретаријата за здравство у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета пружаоца услуга.

Приликом надзора над извршењем квалитета и саобразности уговорене услуге проверава се да ли пружалац услуге задовољава све критеријуме који су били од пресудног значаја приликом избора, укључујући обим и квалитет услуге, као и да се у току поступка извршења услуге може утицати на побољшање квалитета услуге или начина и обима извршења, у складу са утврђеним стварним потребама Покрајинског секретаријата за здравство.

У поступку објективне евалуације квалитета и обима пружене услуге у односу на уговорену, потребно је прикупити све релевантне чињенице, податке и документацију у вези са извршењем услуге, као и прикупити податке од непосредних, крајњих, корисника у вези са предметом услуге. Евалуација се може извршити слањем упитника, разговором са изабраним појединцима или на основу анонимног анкетирања путем елетронске поште.

Управљање променама уговорених услуга од стране пружаоца услуга

Уговором са пружаоцем услуга треба обезбедити могућност континуираног управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контролу безбедности информација.

Промене које се узимају у обзир су промене у споразумима са пружаоцима услуга, повећање обима текућих услуга које се нуде, као и промене које уводи Покрајински секретаријат за здравство ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

27. МЕРА - ПРЕВЕНЦИЈА И РЕАГОВАЊЕ НА БЕЗБЕДНОСНЕ ИНЦИДЕНТЕ, ШТО ПОДРАЗУМЕВА АДЕКВАТНУ РАЗМЕНУ ИНФОРМАЦИЈА О БЕЗБЕДНОСНИМ СЛАБОСТИМА ИКТ СИСТЕМА, ИНЦИДЕНТИМА И ПРЕТЊАМА

Члан 34.

Мера: Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама је у надлежности Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа и регулисано је Упутством о употреби рачунара.

Локални администратор 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 локалног администратора у што краћем року, како би се инциденти нарушавања информационе безбедности спречили и спречио настанак штете.

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.

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.

Одговор на инциденте нарушавања информационе безбедноости

Покрајински секретаријат за здравство је у обавези да усвоји План за превенцију од безбедносних ризика.

Прикупљање доказа

Покрајински секретаријат за здравство дефинише и примењује процедуре за идентификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају покретања дисциплинског, прекршајног или кривичног поступка против лица које је нарушило информациону безбедност ИКТ система.

28. МЕРА - МЕРЕ КОЈЕ ОБЕЗБЕЂУЈУ КОНТИНУИТЕТ ОБАВЉАЊА ПОСЛА У ВАНРЕДНИМ ОКОЛНОСТИМА

Члан 35.

Мера: Мере које обезбеђују континуитет обављања посла у ванредним околностима је у надлежности Управе за заједничке послове покрајинских органа сходно члану 1. и 2. Одлуке о Управи за заједничке послове покрајинских органа.

Имплементација континуитета безбедности информација

У ванредним околностима поступајући по инструкцијама Управе за заједничке послове покрајинских органа запослени примењују мере које обезбеђују континуитета безбедности информација и континуитет обављања посла, као и мере за опоравак ИКТ система од нежељених догађаја, како би ИКТ систем у што краћем року био у функционалном стању.

III ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Покрајинског секретаријата за здравство

Члан 36.

Обавеза Покрајинског секретаријата за здравство је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене овог правилника, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Покрајинског секретаријата за здравство.

Ступање на снагу овог правилника

Члан 37.

Термини који се користе у овог правилника, а који имају родно значење, изражени у граматичком мушком роду, подразумевају природни женски и мушки пол лица на које се односе.

Овај овог правилника ступа на снагу осмог дана од дана објављивања на огласној табли Покрајинског секретаријата за здравство.

ПОКРАЈИНСКИ СЕКРЕТАР ЗА ЗДРАВСТВО
Проф. др Зоран Гојковић

Република Србија
Аутономна покрајина Војводина
Покрајински секретаријат за здравство
Нови Сад
Szerb Köztársaság
Vajdaság Autonóm Tartomány
Tartományi Egészségügyi Titkárság
Újvidék
Srbská republika
Autonómna pokrajina Vojvodina
Pokrajinský sekretariát zdravotníctva
Nový Sad
Република Србиа
Аутономна Покрајина Војводина
Покрајински секретаријат за здравство
Нови Сад
Republika Srbija
Autonomna Pokrajina Vojvodina
Pokrajinsko tajništvo za zdravstvo
Novi Sad
Republica Serbia
Provincia Autonomă Voivodina
Secretariatul Provincial pentru Sănătate
Novi Sad

Правилник је објављен на огласној табли
Покрајинског секретаријата за здравство
дана 29.4.2024. године

Правилник је објављен на интернет презентацији
Покрајинског секретаријата за здравство
Дана 29.4.2024. године