На основу члана 6а став 3. и члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/2016, 94/2017 и 77/2019), члана 2. и 3. Уредбе о ближем садржају акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја („Службени гласник РС”, број 94/2016), Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја („Службени гласник РС“, бр. 94/2016), члана 28. Закона о министарствима („Службени гласник РС“, бр. 128/2020), члана 5. Закона о метеоролошкој и хидролошкој делатности („Службени гласник РС”, број 88/2010), Директор, дана . . 2021. доноси

Акт о безбедности информационо-комуникационог система Републичког хидрометеоролошког завода

РЕПУБЛИКА СРБИЈА
РЕПУБЛИЧКИ ХИДРОМЕТЕОРОЛОШКИ ЗАВОД
Бр. 095-1/2021-2
11 AUG 2021 20 год.
БЕОГРАД

I. ОСНОВНЕ ОДРЕДБЕ

Предмет Акта
Члан 1.

Актом о безбедности информационо-комуникационог система (у даљем тексту: Акт о безбедности) Републичког хидрометеоролошког завода (у даљем тескту: РХМЗ), у складу са Законом о информационој безбедности („Службени гласник РС”, број 6/2016, 94/2017 и 77/2019, у даљем тексту: Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система РХМЗ-а.

Циљеви Акта о безбедности
Члан 2.

Циљеви доношења Акта о безбедности су:

1) одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности ИКТ 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 Акта о безбедности
Члан 3.

Мере заштите ИКТ система дефинисане у Акту о безбедности служе да уклоне или умање вероватноћу настанка инцидената и / или ниво штете од инцидента и њихова примена је обавезна за све запослене у РХМЗ-у.

Запослени у РХМЗ-у морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са:

- одредбама Акта о безбедности,
- одредбама Правилника о мерама које се предузимају у циљу заштите хидрометеоролошког информационог система, као и
- свим другим интерним и екстерним документима који регулишу информациону безбедност у РХМЗ-у или представљају обавезу за усклађивање.

Помоћници директора, начелници, шефови и руководиоци, осим обавезе да непосредно примењују мера заштите у свом раду, имају крајњу одговорност за праћење примене мера безбедности, као и за проверу да ли су информације заштићене на начин који је утврђен Актом о безбедности и другим интерним правилима у оквиру својих организационих јединица.

Одговорност запослених

Члан 4.

Запослени у РХМЗ-у су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу претпостављене и именована лица о свим сигурносним инцидентима и проблемима.

Непоштовање одредби Акта о безбедности, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

Предмет заштите

Члан 5.

Предмет и подручје примене Акта о безбедности и мера заштите ИКТ система односе се на целу организацију РХМЗ-а и обухвата исте процесе и услуге који су дефинисани као предмет и подручје примене система менаџмента квалитетом унутар Пословника о квалитету, укључујући Сектор одбране од града и Одељење за матирајално и финансијско пословање.

Информациона имовина која је обухваћена напред наведеним предметом и подручјем примене Акта о безбедности документује се у регистру информационе имовине који води и одржава РХМЗ. Информациона имовина обухвата хардвер и софтвер, податке и информације, организациону структуру и људске ресурсе, техничку и корисничку документацију, као и помоћне системе и услуге који омогућавају рад ИКТ система.

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.

Организациона структура представља скуп задатака и овлашћења којим се уређује начин на који запослени обављају своје активности и користе расположиве ресурсе за

постизање циљева организације. Републички хидрометеоролошки завод у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

Интерни акти који уређују одговорности и овлашћења у вези са радним операцијама и информационом безбедношћу су:

- Правилник о организацији и систематизацији радних места;
- Уговори о раду;
- Процедуре и упутства система менаџмента квалитетом;
- Изјаве о поверљивости;
- Уговори о чувању поверљивости са правним лицима;
- Правилник о мерама које се предузимају у циљу заштите хидрометеоролошког информационог система;
- Друге обавезе за усклађеност које је РХМЗ преузео у складу са важећим законским прописима – сарадња са Војском Републике Србије, штабовима за кризне ситуације, другим државним органима и сл.

Директор одобрава, у складу са актом о систематизацији, документ Организација информационе безбедности у РХМЗ-у којим одређује Тим за информациону безбедност, Координатора тима за информациону безбедност, Координатора за инциденте, одговорна лица за обезбеђивање и праћење безбедности информационог система РХМЗ-а и лица са одговорностима и овлашћењима специфичним за област информационе безбедности.

У складу са законом о државним службеницима утврђена је одговорност сваког запосленог и одговорног лица и прописује се дисциплинска одговорност, у случају непоштовања одредби које уређују информациону безбедност.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 7.

РХМЗ дозвољава рад на даљину и употребу мобилних уређаја од стране запослених лица, 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 или ангажовање запослених лица за обављање послова ван просторија послодавца обухвата:

- Рад на даљину;
- Рад од куће;
- Виртуелно радно окружење.

Рад на даљину се, где је и када је то потребно, омогућава путем VPN (VPN –virtual private network, тј. виртуална приватна мрежа) приступа и примењује се како на запослене, тако и на сараднике.

Овим се своди на минимум потенцијална изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи ИКТ система.

Захтеви који морају бити испуњени и дефинисани у VPN процедури:

1. Приступ са удаљених локација мора бити заштићен коришћењем криптографских алгоритама.
2. Ауторизовани корисници морају чувати креденцијале својих налога и не смеју омогућити приступ било ком трећем лицу.
3. Приликом коришћења службеног рачунара за приступ са удаљене локације мрежи РХМЗ-а ауторизовани корисник не сме истовремено бити повезан и на неку другу мрежу која може угрозити безбедност комуникације.
4. Приступ са удаљене локације мора бити одобрен од стране одговорног лица за надзор спровођења VPN процедуре.
5. Сви уређаји који су повезани на интерну мрежу преко удаљених локација морају имати инсталирану заштиту у виду антивирусног софтвера. Трећа лица су у обавези да примењују захтеве из закључених уговора са РХМЗ-ом.
6. Сви пословни подаци који се креирају приликом рада на даљину складиште се у информационом систему. Ради безбедности, пословни подаци се не складиште на мобилним уређајима.

Рад на даљину одобрава Помоћник директора за конкретан сектор, односно надлежни руководилац за унутрашњу организациону јединицу изван сектора, уз консултације са Тимом за информациону безбедност.

Коришћење мобилних уређаја

Мобилни уређаји подразумевају преносиве рачунаре, таблете, мобилне телефоне, PDA (Personal Digital Assistant, тј. лични дигитални помоћник) и све друге мобилне уређаје који садржи податке и имају могућност повезивања на мрежу.

Следећа правила се морају поштовати тамо где је то процењено као потребно:

1. Сви уређаји морају бити заштићени јаком шифром – 8 или више карактера (слова – велика и мала, бројеви, специјални знакови).
2. Мора бити инсталирана антивирусна заштита.

Правила се примењују на све стално запослене, запослене на одређено време или лица ангажована по другим основима, који имају приступ или користе мобилне уређаје у власништву РХМЗ-а.

Право на коришћење мобилних уређаја ван седишта РХМЗ-а се стиче на основу захтева и потреба радног места, а по одобрењу Помоћника директора за конкретан сектор и консултација са Тимом за информациону безбедност.

Десктоп рачунари, када се користе за рад на даљину, морају имати примењене најмање исте безбедносне мере као и сродни уређаји који се налазе у оквиру мреже, док се за заштиту комуникације морају применити исте мере као и за заштиту комуникације мобилних уређаја.

Евиденцију о уређајима намењеним за рад на даљину у оквиру сектора води Помоћник директора, односно надлежни руководилац за унутрашњу организациону јединицу изван сектора, а обједињену евиденцију води Тим за информациону безбедност.

Евиденција о уређајима треба да садржи податке који су неопходни да би се уређај и/или корисник недвосмислено идентификовали.

Корисник мобилног уређаја у обавези је да крађу или губитак мобилног уређаја пријави без одлагања непосредном руководиоцу и Помоћнику директора. По пријави крађе или губитка мобилног уређаја, неодложно се блокира несталом мобилном уређају приступ информационом систему и кориснику се мењају креденцијали за приступ.

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.

РХМЗ 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.

Провера кандидата и услови запошљавања

РХМЗ, у складу са важећим прописима и захтевима радног места, спроводи провере испуњености услова сваког појединачног кандидата за запослење.

Сви запослени и радно ангажовани појединци по другом основу којима је додељен приступ поверљивим информацијама, морају потписати споразум о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Обавезе у току запослења

Руководство РХМЗ-а је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

РХМЗ 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 и у континуитету;
- Штити информације и податке са сличним профилом осетљивости и карактеристика 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.

Сви чланови Тима за информациону безбедност континуирано се обучавају у циљу унапређења техничког и технолошког знања. Тим за информациону безбедност је ауторизован за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Упознавање са безбедношћу информација, стицање знања и обука

Сви запослени у РХМЗ-у су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Дисциплински поступак

Дисциплински поступак се спроводи ради предузимања процесних и других материјалних радњи и поступака против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и у примени код РХМЗ-а.

Дисциплински поступак се спроводи у складу са Правилником о дисциплинском поступку.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код РХМЗ-а

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 запослења треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа.

Ова мера је ближе одређена документима:

- Уговор о раду и
- Споразумом о поверљивости

али не искључује и друге документе према потреби.

За поступања приликом престанка запослења или ангажовања задужено је Одељење за опште, правне и персоналне послове, које 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 РХМЗ-а 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 РХМЗ-а.

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 као и друге ресурсе дефинисане чланом 5. Акта о безбедности.

Пописивање имовине

РХМЗ врши идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација. РХМЗ прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Регистар информационих ресурса по секторима воде Помоћници директора, односно надлежни руководиоци за унутрашње организационе јединице изван сектора, а обједињен регистар води Тим за информациону безбедност. Помоћник директора, односно надлежни руководилац унутрашње организационе јединице изван сектора, након прегледа регистра за свој сектор/организациону јединицу, непосредно ажурира обједињен регистар са подацима свог сектора/организационе јединице или обавештава Координатора тима за информациону безбедност који даље одлучује о начину ажурирања обједињеног регистра.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај

Појединци којима је дата одговорност за контролисање животног циклуса имовине дужни су за правилно управљање имовином током целог животног циклуса.

РХМЗ дефинише правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација.

Запослени и екстерни корисници су обавезни да врате сву имовину РХМЗ-а коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

Током отказног рока запослених, РХМЗ контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком 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 РХМЗ.

РХМЗ означава типове и локације података као поверљиве, интерне или јавне. Имовина се означава уз помоћ идентификационих налепница које носе одговарајућу класификациону ознаку.

РХМЗ класификациону шему поверљивости информација базира 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, угрожава опстанак или представља одавање државне тајне.

РХМЗ врши класификацију ради:

- Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и буду свесни одговорности за неовлашћено коришћење или преношење;
- Подизања свести о вредности информације или документа;
- Заштите садржаја;

Класификација документа мора да буде усклађена са правилима контроле приступа.
РХМЗ поступања у складу са усвојеном Шемом класификовања података.
РХМЗ у свом раду примењује:

- ограничења приступа у складу са нивоом 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.

Заштита носача података
Члан 12.

РХМЗ обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, води Помоћник директора за конкретан сектор, односно надлежни руководилац за унутрашњу организациону јединицу изван сектора, у оквиру регистра информационих ресурса.

Управљање преносним носачима података

РХМЗ је за управљање преносним носачима података примњеује поступак у складу са усвојеном Шемом класификовања података:

- 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 сачинити запис, 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;

Расходовање носача података

Када више нису потребни, медијуми се морају расходовати на безбедан начин.

РХМЗ врши безбедносно расходовање медијума уз свођење на минимум ризика од доступности осетљивих информација неовлашћеним особама.

Медијуме који садрже осетљиве информације треба расходовати спаљивањем или кидањем, или брисањем података ради коришћења у неком другом апликативном програму унутар организације;

Физички пренос носача података

Носачи података који садрже информације се штите од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта. Када поверљива информација на медијуму није шифрована, потребно је додатно физички заштити медијум.

Ограничење приступа подацима и средствима за обраду података

Члан 13.

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.

РХМЗ је утврдио попис свих информационих ресурса којима се мора ограничити приступ и лица која им могу приступити.

Корисницима је дозвољен приступ само мрежи и мрежним услугама за коју имају овлашћења да користе.

РХМЗ је уредио приступ мрежи и мрежним уређајима кроз:
- листа мрежа и мрежних услуга којима је приступ дозвољен;
- ауторизацију ради утврђивања коме је одобрен приступ, којој мрежи и којим 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.

РХМЗ управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

Управљање корисничким идентификаторима врши се поштујући следеће принципе:

- кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;
- вишеструки кориснички идентификатори се периодично идентификују и уклањају или онемогућавају;
- 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 Помоћника директора за тај сектор.

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

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

Шифре за приступ општим корисничким идентификаторима администратора мењају се променом корисника.

РХМЗ једном годишње врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај запослења).

Запосленима лицима 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 јединственог корисничког имена и шифре.

Сви корисници су дужни да:

- корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
- промене шифру увек када постоји било какав наговештај могућег компромитовања.

Шифре морају да:

- Садрже најмање 8 алфанумеричких карактера
- Садрже најмање једно велико и једно мало слово
- Садрже најмање 1 број (0-9)
- Сардже један специјални карактер (# % & * и сл.)

Шифре не смеју бити засноване на личним података особе, као што су име, телефонски број или датум рођења. У себи не смеју да садрже више од 3 узастопна идентична бројчана или словна знака.
Корисници су дужни да привремене шифре промене приликом првог пријављивања. Шифре се периодично мењају на 90 дана.

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

Члан 16.

У циљу заштите података РХМЗ користи криптографске контроле у виду VPN за рад са удаљене локације и SSL (Secure Socket Layer) сертификате за рад са електронском поштом.

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

Члан 17.

РХМЗ је дужан да предузме мере ради спречавања неовлашћеног физичког приступа својим објектима и зонама унутар објеката, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација и опреме за обраду информација.

Зона раздвајања и успостављање система физичке безбедности

Опрема за обраду информација се штити закључавањем просторија у којима се налази.

У складу са проценом ризика дефинисане су следеће зоне раздвајања: рестриктивна зона – сервер сале, архива, канцеларије руководства; интерна зона (само за запослене) – радне просторије, складишта, слободна зона – пријемни простор, холови и сл.

Контрола физичког уласка

Безбедне области морају бити заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ, складу са смерницама.

У РХМЗ се спроводи:

- евиднетирање датума и времена уласка и изласка посетилаца, а све посетиоце треба надгледати, осим ако њихов приступ није претходно одобрен; приступ треба одобравати само за специфичне, ауторизоване сврхе и треба издавати упутства о захтевима за безбедност области и о процедурама за ванредне ситуације;
- приступ областима у којима се обрађују или чувају поверљиве информације треба да буде ограничен само на овлашћене особе, применом одговарајућих контрола приступа, нпр. имплементацијом двофакторских механанизама за проверу веродостојности, као што су картице за приступ и тајни лични идентификациони број (PIN - Personal Identification Number);
- треба безбедно одржавати и надгледати физичку књигу записа или електронски траг провере свих приступа;
- од свих запослених, уговарача и треће стране, као и од свих посетилаца треба захтевати да носе неку форму видљиве идентификације и да одмах известе особље обезбеђења уколико наиђу на посетиоце без пратиоца или примете било коју другу особу која не носи видљиву идентификацију;
- запосленима код пружаоца услуга обезбеђења треба одобрити ограничен приступ безбедним областима или опреми за обраду осетљивих информација и само онда када је то потребно; овакав приступ треба да буде одобрен и надгледан у сваком тренутку;
- права приступа безбедним областима треба редовно преиспитивати и ажурирати, као и укидати их када је потребно.

Заштита канцеларија, просторија и средстава и заштита од претњи екстерних фактора из окружења

РХМЗ примењује инструменте за обезбеђивање физичке безбедности канцеларија, просторија и средстава, тако што се онемогућава јавни приступ кључној опреми, конфигурисањем средстава у циљу спречавања видљивости поверљивих информација и активности споља. Физичка заштита се мора планирати и за случајеве природних катастрофа, непријатељских напада или несрећа.

Рад у безбедним областима

Безбедне области подлежу следећим мерама заштите:

- особље мора бити обавештено о постојању и активностима унутар безбедне области;
- забрањује се рад без надзора у безбедним областима;
- безбедне области које се не користе морају бити физички закључане и периодично преиспитиване;
- не дозвољава се уношење фотографских, видео, аудио или других уређаја за записивање, осим уз претходно одобрење одговорног лица.

Евиденцију о уласку у безбедносну област води одговорно лице за конкретан сектор.

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 могућности за неовлашћени приступ.

Превенција за безбедност опреме:

- Опрема се поставља на месту који 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 особама које нису овлашћене;
- Врши се редовна контрола система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, гас, електронске комуникације;
- 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;

Лица одговорна за сервер сале редовно прате услове околине, као што су температура и влажност, који би могли негативно да утичу на рад опреме за обраду информација.

Помоћне функције за подршку

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.

Безбедносни елементи приликом постављања каблова

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од ометања или оштећења на следећи начин:

- водови напајања и телекомуникациони водови који улазе у просторије за обраду информација су подземни, онда када је то могуће, или имају адекватну алтернативну заштиту;
- каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње;
- за осетљиве или критичне системе се постављају оклопљени водови, користе закључане просторије или кутије, електромагнетско оклапање ради заштите каблова;
- неовлашћено прикључење уређаја на каблове се врши техничким претраживањем и физичком провером;
- приступ до разводних табли и у просторије са кабловима се контролише.

Одржавање опреме

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;
- о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;
- осетљиве информације треба избрисати из опреме;
- пре враћања опреме у рад након одржавања, треба је прегледати да би се уверили да није неовлашћено коришћена или оштећена.

Измештање и премештање имовине

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 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.

Безбедност измештене опреме и имовине

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

Безбедно расходовање или поновно коришћење опреме

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

Безбедност опреме корисника без надзора

Корисници треба да осигурају 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:

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. Носиоци података као што су дискови и flash меморија морају бити одложени и закључани.
5. Шифре за приступ не смеју бити написане и остављене на приступачном месту.
6. Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.
7. Материјал који је намењен за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Усвајање и примена радних процедура

РХМЗ посебну пажњу поклања извршењу следећих послова:
а) инсталација и конфигурација система;
б) обраду и поступање са информацијама (аутоматски и мануелно);
в) израда резервних копија;
г) захтеви за временски распоред активности;
д) инструкције за поступање према грешкама или другим ванредним стањима која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција;
ђ) контакти за подршку (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;
е) инструкције за поступања према поверљивим подацима;
ж) процедуре за поновно покретање система и опоравак, које се користе у случају отказа система;
з) управљање информацијама о трагу провере система и системским записима (логовима);
и) процедуре за надгледање.

Усвајање, измене и допуне радних процедура дефинисани су Процедуром за управљање документованим информацијама.

Управљање расположивим капацитетима

Коришћење ресурса се надгледа, подешава и пројектује у складу са захтеваним капацитетима у наредном периоду, како би се осигурале захтеване перформансе система. Периодично се спроводе следеће активности:
а) брисање застарелих података (простора на диску);
б) повлачење из употребе апликација, система, база података или окружења;
в) оптимизација серије процеса и распореда;
г) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису критичне за пословање.

Раздвајање окружења за развој, испитивање и рад

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

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 20.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен или неумрежен рачунар. Заштита од злонамерног софтвера се заснива на софтверу за откривање злонамерног софтвера и отклањање штете, на познавању безбедности информација, као и на одговарајућим контролама приступа систему и управљања захтеваним и потребним променама.

Поступак контроле и предузимање мера против злонамерног софтвера

РХМЗ одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Ово обухвата:
1) формална забрана коришћења неауторизованих софтвера;
2) имплементација контрола које спречавају или откривају коришћење познатих или сумњивих компромитованих веб-сајтова;
3) спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе; присуство било каквих неодобрених датотека или неауторизованих допуна треба формално истражити;
4) инсталирање и редовно ажурирање антивирусног и антималверског софтвера и опоравак ради претраживања рачунара и медијума као контролу из предострожности, или на рутинској основи.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави непосредном руководиоцу и Координатору за инциденте.

У циљу заштите, односно упада у ИКТ систем РХМЗ-а са интернета, Одељење за хидрометеоролошки рачунарско-комуникациони систем је дужно да одржава систем за спречавање упада.

Заштита од губитка података

Члан 21.

РХМЗ врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација и података

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

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

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

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

За чување заштитних копија користе се магнетне траке, екстерни хард дискови, CD/DVD медији и системи за архивирање и складиштење података.

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

Члан 22.

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

Записивање догађаја

РХМЗ прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са безбедношћу информација, који се морају чувати и редовно преиспитивати.

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.

Заштита информација у записима

Средства за записивање и записане информације су заштићени од неовлашћеног мењања и приступа.

Забрањено је неовлашћено уношење следећих измена:

- мењање типова порука које се записују;
- уношење измена у датотеке са записима или њихово брисање;
- препуњавање медијума за записе, што доводи до отказа записивања догађаја или уписивања преко већ раније записаног.

Записи администратора и оператора

Активности администратора и оператора система се записују, а записи штите и редовно преиспитују. Власници привилегованих корисничких налога могу бити у стању да управљају записима на опреми за обраду информација која је под њиховом директном контролом, на који начин се штите и прегледају записи да би се одржала одговорност за привилеговане кориснике.

Сатови свих одговарајућих система за обраду информација заштите морају бити синхронизовани по Гриничком средњем времену.

Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

РХМЗ спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система у складу са смерницама 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;
- 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 апликацијског 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 Администратор, односно запослени-корисник који има овлашћење за то.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

РХМЗ 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

РХМЗ 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.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, Администартор је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене рањивости. Прво се узимају у разматрање системи са високим ризиком.

Ограничења у погледу инсталације софтвера

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедносним слабостима.

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

Члан 25.

Приликом спровођења ревизије ИКТ система, РХМЗ обезбеђује да ревизија има што мањи утицај на фукционисање система:

- Са одговарајућим руководством су договорени захтеви за проверу приступа систему и подацима;
- Предмет и подручје испитивања за проверу су унапред договорени и строго контролисани;
- Испитивања за проверу су ограничена на приступ читањем;
- Приступ који није ограничен само на читање треба дозволити само за добијање издвојених копија системских датотека које се по завршеној провери бришу или се одговарајући штите уколико постоји обавеза да се такве датотеке чувају према захтевима за документовање провере;

- Захтеви за посебну или допунску обраду морају бити идентификовани и о томе мора бити сачињен писани споразум;
- Испитивања за проверу могу утицати на доступност система, па се покрећу ван радног времена;
- Сав приступ се надгледа и записује се да би се направио референтни траг.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 26.

У циљу заштите података у комуникационим мрежама, уређајима и водовима врши се њихова контрола и заштита од неовлашћеног приступа.

Мрежама управљају мрежни администратори. У споразуму о мрежним услугама, за све мрежне услуге треба одредити и укључити механизме безбедности, нивое услуга и захтеве за руководство, било да се те услуге пружају унутар организације или из спољног извора. Мрежне услуге обухватају обезбеђивање прикључака, услуге на приватним мрежама и мреже са допуњеним функцијама, као и решења за управљање безбедности, као што су заштитне преграде и системи за откривање упада.

У мрежама су међусобно раздвојене групе информационих услуга, корисника и информациони системи, а мрежни администратор је одговоран за управљање мрежом.

Одељење за техничку инфраструктуру и одржавање објекта је дужано да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

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 РХМЗ-а, 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 правилима поступка, сигурна и у складу са позитивним прописима и пословном праксом. 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. Мрежа користи поступак ревизије логовања, како на пријему тако и на слању, и периодично се надзире и контролише.

- Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намена коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

Споразуми о преносу информација

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

Размена електронских порука

Информације укључене у размену електронских порука се штите кроз:

- заштиту порука од неовлашћеног приступа, модификовања или одбијања услуга које су у складу са класификационом шемом коју је усвојила организација;
- осигурање исправног адресирања и транспорта поруке;
- поштовање законских одредби, на пример захтеве за електронске потписе;
- добијање одобрења пре коришћења јавних спољних услуга, као што су размена хитних порука, приступ и коришћење друштвене мреже или заједничко коришћење датотека;
- строже нивое утврђивања веродостојности, контролисањем приступа из мрежа са јавним приступом.

Споразуми о поверљивости или неоткривању

Споразуми о поверљивости или неоткривању штите информације РХМЗ-а и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

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, РХМЗ је у обавези да обезбеди безбедност информација у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења.

Помоћник директора за конкретан сектор, односно надлежни руководилац за унутрашњу организациону јединицу изван сектора или лице које он одреди из свог сектора/организационе јединице, је задужено за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система Начелник одељења за хидрометеоролошки рачунарско-телекомуникациони систем води документацију.

Анализа и спецификација захтева за безбедност информација

У захтеве за нове информационе системе или за побољшање постојећих информационих система морају бити укључени захтеви који се односе на безбедност информација и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Захтеви за безбедност информација укључују:

- Проверу идентитета корисника;
- Доступност, поверљивост, непорецивост и интегритет података и имовине;
- Надгледање пословних процеса;
- Омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке кориснике.

Спецификација захтева мора узети у обзир аутоматску контролу која ће бити уведена у информациони систем и потребу да такође постоји и ручна контрола, која мора бити примењена при вредновању пакета софтвера, развијених или купљених, за пословне апликације.

Системски захтеви за информациону безбедност и процеси за увођење безбедности се интегришу у фази дизајнирања информационих система.

Формално тестирање и процес имплементације ће се примењивати за све купљене производе.

У уговору са набављачем за купљене производе дефинишу се захтеви безбедности.

У случају да безбедносна функционалност предложеног производа не задовољава одређен захтев, ризик и повезане контроле ће бити преиспитане пре куповине производа.

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 потврдити идентитет корисника и извршити поделу овлашћења и одговорности за постављање садржаја, електронског потписивања или обављања трансакција.

Заштита трансакција апликативних услуга

Информације укључене у трансакције апликативних услуга се штите да би се спречио непотпун пренос, погрешно усмеравање, неовлашћено мењање порука, неовлашћено разоткривање, неовлашћено копирање порука или поновно емитовање.

Трансакције, у зависности од врсте и важности, могу да подрже следеће услове:

- Обе стране које учествују у транскакцији морају да примене електронски потпис;
- Приватност свих страна које учествују у трансакцији;
- На комуникационим каналима примењено шифровање;
- Безбедност протокола који се користе у трансакцијама.

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, РХМЗ не користи оперативне податаке 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.

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 РХМЗ-а 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 са РХМЗ-ом.

РХМЗ успоставља контролу безбедности информација које се односе на процесе које ће спроводити пружаоци услуга кроз:

- идентификовање и документовање врсте пружаоца услуга којима ће се 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.

Уговорање обавезе обезбеђивања безбедности у споразумима са пружаоцима услуга

Пре отпочињања преговора, 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 РХМЗ-а и за потребе извршења предмета преговора.

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 РХМЗ-а у случају њене повреде.

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

Члан 31.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, РХМЗ успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга

Помоћник директора за конкретан сектор, односно надлежни руководилац за унутрашњу организациону јединицу изван сектора, или одговорно лице из сектора/организационе јединице, редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

- Надгледање и преиспитивање услуга се може вршити преко трећег лица;
- Неопходно је да се поштују сви услови из споразума у вези са безбедношћу информација, као и да се спрече сви инциденти и проблеми нарушавања безбедности, те омогући управљање на одговарајући начин;
- Врши се оцена квалитета извршења и саобразности уговорене услуге;
- Пружалац услуге има уговорну обавезу да организује и припреми периодичне састанаке који ће обезбедити редовно извештавање РХМЗ-а и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка

примене;

- Помоћник директора за конкретан сектор, односно надлежни руководилац за унутрашњу организациону јединицу изван сектора, или одговорно лице из сектора/организационе јединице одржава потпуну контролу над спровођењем услуга и осигурава увид у све осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа страна приступа, процесира или којима управља;
- Помоћник директора за конкретан сектор, односно надлежни руководилац за унутрашњу организациону јединицу изван сектора, или одговорно лице из сектора/организационе јединице одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања;
- Преиспитује трагове провере и записа о догађајима у вези са безбедношћу код пружаоцем услуга, оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене; утврдити поступак извештавања, праћења и поступања у складу са захтевима РХМЗ-а 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 РХМЗ-а.

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 и прикупљање података 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 електронске 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 РХМЗ ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

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

РХМЗ одређује Координатора за инциденте чији је задатак да придржавајући се процедура одређених овим чланом, планира, детектује, анализира и информише надлежне у току и након инцидента.

Координатор за инциденте у циљу превенције обезбеђује мехнизам за комуникацију и координацију у случају нарушавања безбедности:
обезбеђивање контакта информација (број телефона, електронска адреса) појединаца и чланова тима у оквиру организације и ван ње, систем за праћење проблема, шифорвани софтвер који би био коришћен од стране појединаца у оквиру организације и спољашних странака, посебну осигурану просторију за чување података и скадиштење поверљивог материјала.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести непосредног руководиоца и Координатора за инциденте.

Извештавање о догађајима у вези са безбедношћу информација

Сви запослени морају бити упознати са обавезом и поступком извештавања о догађајима у вези са безбедношћу информација.

Координатор за инциденте је у дужан да припреми план и начин комуникације које би могле да се примене у зависности од инцидента (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 безбедношћу информација.

Када је индетификован инцидент запослени је дужан да одмах обавести непосредног руководиоца и Координатора за инциденте, и предузме мере у циљу заштите ресурса ИКТ система.

Координатор за инциденте 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 извештавају о уоченим и утврђеним слабостима ИКТ система Координатора за инциденте, у што краћем року, како би се инциденти нарушавања безбедности информација спречили 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 безбедношћу информација се оцењују и у складу са тим се доноси одлука да ли је потребно да се класификују као инциденти нарушавања безбедности информација.

Одговор на инциденте нарушавања безбедности информација

РХМЗ је у обавези да усвоји План за превенцију безбедносних инцидената.

План за превенцију безбедносних ризика садржи одговоре на питања ко треба да буде контактиран, када и како и које акције треба предузети моментално у случају одређеног напада

Прикупљено знање из анализе и решавања инцидената који су нарушили безбедност информација, РХМЗ користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

Прикупљање доказа

РХМЗ идентификује, сакупља и чува информација које могу да служе као доказ у случају покретања казнених мера унутар организације.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

РХМЗ 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 сервера.

План за обезбеђење континуитета пословања за хардверске компоненте ИКТ система обухвата 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.

План опоравка од нежељених догађаја ИКТ сервера обухвата:
- процена најкритичније апликације, података, конфигурационих фајлова и системских софтвер за који треба направити резервне копије;
- место чувања копије;
- податак о новој локацији рада ИКТ сервера у случају немогућности рада на основној локацији/ избор рачунара који ће привремено заменити сервер док се сервер не стави у функцију.;
- подаци о тиму који ће бити ангажован на отклањању последица нежељених догађаја;
- извор непрекидног напајања електричном енергијом.

Плана опоравка од нежељених догађаја ИКТ сервиса и апликација предвиђа:
- 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, РХМЗ примењује процедуре и контроле описане у Плану за обезбеђење континуитета пословања.

РХМЗ редовно врши проверу усвојених процедура контроле континуитета безбедности информација, како би оне биле важеће 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. ПРЕЛАЗНА И ЗАВРШНА ОДРЕДБА

Посебна обавеза РХМЗ-а
Члан 34.

Обавеза РХМЗ-а 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 РХМЗ-а.

Ступање на снагу Акта о безбедности
Члан 35.
Овај Акт о безбедности ступа на снагу 11. 8. 2021. године.

ДИРЕКТОР

Проф. др Југослав Николић, дипл. мет.