РЕПУБЛИКА СРБИЈА
ДИРЕКЦИЈА ЗА ЖЕЛЕЗНИЦЕ
I-02 број: 86/2020
Дана: 14. јануара 2020. године
Београд, Немањина бр. 6.

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16 и 94/17 и 77/2019), 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), Закона о државној управи („Службени гласник РС”, бр.79/2005, 99/2014, 47/2018 и 30/2018- др.закон), в.д. Директора Дирекције за железнице доноси

Акт о безбедности информационо-комуникационог система Дирекције за железнице

ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система (у даљем тексту: Акт о безбедности), у складу са Законом о информационој безбедности („Службени гласник РС”, број 6/16, 94/17, 77/2019 у даљем тексту: Закон), 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 Дирекције за железнице (у даљем тексту: Дирекција).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

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

ресурсима ИКТ система;

5. свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Акта о безбедности

Члан 3.

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

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

Непосредни руководиоци одговорни су за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност запослених

Члан 4.

Запослени у Дирекцији су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу правно лице за информационо технолошке послове 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.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Предмет заштите је имовина пописана Прилогом 1 – Списак опреме и софтвера, Уговора о одржавању рачунарског система са правним лицем за информационо технолошке послове.

МЕРЕ ЗАШТИТЕ

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање

информационом безбедношћу у оквиру Дирекције

Члан 6.

Дирекција Уговором о одржавању рачунарског система са правним лицем за информационо технолошке послове утврђује послове и одговорности у циљу управљања информационом безбедношћу.

Интерни акти који уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу су:

- Правилник о унутрашњем уређењу и систематизацији радних места;
- Директива о поступању запослених и радно ангажованих лица у Дирекцији у циљу заштите информационо-комуникационог система.

Директор Дирекције за железнице (у даљем тексту: Директор) посебним решењем/уговором са правним лицем за информационо технолошке послове одређује лица одговорна за обезбеђивање и праћење безбедности информационог система.

Директор утврђује начин доделе овлашћења за приступ ИКТ систему, степен обуке и квалификацију запослених, начин одобравања приступа запосленима од стране руководиоца, односно непосредно надређеног лица.

Сви запослени морају бити упознати са процедуром заштите безбедности ИКТ система. Сваки запослени и одговорно лице који се не буде придражвало упустава, биће опомену од стране стручних лица, а уколико буде наставило да не поштује упуства, биће санкционисано сходно Закону о државним службеницима.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 7.

У Дирекцији се не обавља рад на даљину, нити се послови Дирекције обављају путем мобилних уређаја.

Сви послови Дирекције обављају се искључиво у просторијама Дирекције и искључиво на уређајима који су власништву Дирекције и који се налазе у њеним пословним просторијама.

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.

Дирекција је у обавези да се стара да запослени/правно лице за информационо технолошке послове које управља ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају. Њихове одговорности су утврђене у складу са Законом о државним службеницима, Законом о раду и интерним актима.

Провера кандидата и услови запошљавања

Приликом спровођења јавног или интерног конкурса, као и ангажовања запослених на одређено време по другим основама, Дирекција врши проверу испуњености услова сваког појединачног кандидата, у складу са одговарајућим прописима и етичким

правилима, сразмерно пословним захтевима, класификацији информација којима ће имати приступ и сагледаним ризицима.

Сви запослени и радно ангажовани по другом основу, морају са поверљивим информацијама поступати у складу са Законом о државним службеницима, Законом о раду и интерним актима.

Обавезе у току запослења

Руководство Дирекције дужно је да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом.

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

- обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;
- штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама;
- спроводи програме заштите на конзистентан и уједначен начин у свим организационим јединицама;
- координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

Правно лице за информационо технолошке послове одговорно је за обезбеђивање и праћење безбедности информационог система.

Правно лице за информационо технолошке послове је фирма коју Дирекција ангажује на основу уговора ради одржавања рачунарске мреже, као и ради свих осталих послова повезаних са рачунарском мрежом у Дирекцији.

Правно лице за информационо технолошке послове ауторизовано је 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 Дирекцији 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 против запослених који су нарушили безбедност информација или на други начин извршили повреду правила Дирекције, покреће се и спроводи у складу са Законом о државним службеницима.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених у Дирекцији

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, и након престанка или промене радног ангажовања.

Приликом престанка запослења или ангажовања Одељење за регулисање железничког тржишта, лиценце, права путника и заједничке уз стручну помоћ правног лица за информационо технолошке послове предузима следеће активности:

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату,
- 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 правном лицу за информационо технолошке послове за укидање налога електронске поште и свих других права приступа систему Дирекције на дан престанка радног односа или другог основа ангажовања бившег запосленог,
- прегледа све налоге и приступе систему који су били доступни запосленом,
- 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 Дирекције.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра у Дирекцији обухватају податке у датотекама и базама података, конфигурацију хардверских компоненти, техничку и корисничку документацију и унутрашње акте.

Пописивање имовине

Евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води правно лице за информационо технолошке послове у сарадњи са Одељењем за регулисање железничког тржишта, лиценце, права путника и заједничке послове.

Власништво над имовином, правилно коришћење имовине и њен повраћај

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

Дирекција уређује правила за правилно коришћење имовине повезане са информацијама и опремом за обраду информација.

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

Током отказног рока запослених, Дирекција 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 података је поступак утврђивања и појединачног додељивања нивоа тајности података, у складу са њиховим значајем за Дирекцију.

Постојећи подаци у Дирекцији су класификовани као интерни и јавни, изузев података који су регулисани Законом о заштити података о личности.

Заштита носача података

Члан 12.

Дирекција обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, води овлашћено правно лице за информационо технолошке послове.

Управљање преносним носачима података (медијумима)

Управљање преносним носачима подразумева следеће:

- садржај сваког медијума који се може поново користити и који ће се износити изван Дирекције, онда када више није потребан, треба да се неповратно избрише;
- за све медијуме који се износе из Дирекције, онда када је то неопходно и изводљиво, треба захтевати одобрење, а о свим таквим изношењима треба водити евиденцију, како би се сачувао траг за проверу;
- све медијуме треба складиштити на безбедном и заштићеном месту, у складу са препорукама произвођача;
- подаци треба да буду пренети на нови медијум пре него што постану нечитљиви;
- вишеструке копије вредних података треба чувати на одвојеним медијумима да би се додатно смањио ризик од случајног оштећења или губитка података;
- да би се ограничила могућност губљења података, треба предвидети регистровање преносних медијума;
- покретне преносне медијуме треба користити само ако за то постоји пословна потреба;
- уколико постоји пословна потреба за коришћењем преносних медијума, неопходно је пратити пренос података на такве медијуме.

Расходовање носача података (медијума)

Када више нису потребни, медијуми се расходују на безбедан начин. Расходовање медијума на безбедан начин Дирекција врши свођењем на минимум ризика од могућег

преузимања осетљивих података од стране неовлашћених особа.

За безбедно расходовање медијума који садрже поверљиве податке утврђују се различити начини процеса расходовања, а у складу са осетљивошћу података.

Безбедно расходовање медијума подразумева следеће:

- неопходно је уредити начин за идентификовање медијума који садрже осетљиве податке за које ће можда бити потребно безбедносно расходовање;
- медијуме који садрже осетљиве податке треба расходовати спаљивањем или кидањем, или брисањем података ради коришћења у неком другом апликативном програму унутар организације;
- расходовање медијума који садрже осетљиве податке је потребно евидентирати, како би се сачувао траг за проверу.

Физички пренос носача података (медијума)

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.

Безбедан транспорт подразумева:

1. поуздани транспорт и курире;
2. потребно је увести проверу идентитета курира;
3. карактеристике опреме за пренос морају да буду такве да обезбеде заштиту од свих физичких оштећења која би могла настати током преноса.

У случају транспорта носача података са информацијама, Дирекција одређује лице које ће вршити транспорт и начин транспорта.

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.

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

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

Члан 14.

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

Управљање корисничким идентификаторима врши се уз поштовање следећих принципа:

- кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- коришћење заједничких идентификатора дозвољава се само онда када је то погодно

за обављање посла уз претходно одобрење;

- корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;
- периодично се врши идентификовање и уклањање или онемогућавање вишеструких корисничких идентификатора;
- вишеструки идентификатори неког корисника се не издају другим корисницима.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Додељивање привилегованих (администраторских) права на приступ врши се на основу одлуке Директора.

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

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

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

Дирекција једном годишње врши преиспитивање права корисника на приступ, као и након сваке промене кретања у служби.

Запосленима, другим радно ангажованим и екстерним корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15.

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

Сви корисници су дужни да:

- корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
- избегавају чување корисничког имена и шифре у писаном облику;
- промене шифру када примете да постоји било какав наговештај могућег компромитовања.

Шифре морају да:

- садрже најмање 9 алфанумеричких карактера;
- садрже најмање једно велико и једно мало слово;

- садрже најмање 1 број (0-9).

Шифре не заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и не смеју садржати више од 3 узастопна идентична бројчана или словна знака.

Корисници су дужни да привремене шифре промене приликом првог пријављивања.

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

Члан 16.

Приступ ресурсима ИКТ система Дирекције не захтева криптозаштиту.

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

Члан 17.

Дирекција је дужна да предузме мере ради спречавања неовлашћеног физичког приступа просторијама, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација.

Зона раздвајања и успостављање система физичке безбедности

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

Зоне раздвајања у згради или на локацији која садржи опрему за обраду информација треба да буду физички исправне (тј. не треба да постоје процепи у зони или области у којој би се лако могао десити упад); спољни кров, зидови и подови на тој локацији треба да буду од чврстог материјала, а сва спољна врата треба да буду потпуно заштићена од неовлашћеног приступа помоћу контролних механизама, нпр. врата и прозори треба да буду закључани а у свим случајевима када су без надзора, а када су у питању прозори, треба размотрити спољну заштиту, посебно у приземљу.

Опрема за обраду информација којом управља организација треба да буде физички одвојена од оне којом управљају трећа лица.

Контрола физичког уласка

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

Контролу уласка у просторије Дирекције врше лица које су задужена за обезбеђење целе пословне зграде у којој,ј поред Дирекције, послове обављају и друга правна лица.

Рад у безбедносним зонама

Дирекција не обавља послове у просторијама које се сматрају безебедоносним зонама у смислу Закона о информационој безбедности.

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

Члан 18.

Постављање и заштита опреме

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

Безбедност опреме:

- опрема се поставља на месту које се може обезбедити од неовлашћеног приступа;
- опрема за обраду информација која служи за приступ и коришћење осетљивих података се поставља на места која нису видљива неовлашћеним особама;
- редовну контролу система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, гас, електронске комуникације, врши управа пословне зграде;
- просторије са опремом се редовно чисте од прашине;
- забрањено је конзумирање хране и пића и пушење у близини опреме за обраду информација;
- опрема мора бити заштићена од атмосферских падавина.

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 се редовно процењује;
- опрема редовно прегледа и испитује у погледу правилног функционисања и врши се поправка кварова;

Безбедносни елементи приликом постављања каблова

Каблови за напајање и телекомуникациони каблови су у надлежности управе пословне зграде.

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од прислушкивања, 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 се закључане просторије или кутије и примењује се 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;
- осетљиве информације треба избрисати из опреме;
- пре враћања опреме у рад након одржавања, потребно ју је прегледати како би се проверило 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 спроведу измештање имовине;
- треба да се поставе временска ограничења за измештање опреме и да се проверава усклађеност приликом повратка;
- треба документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања и ова документација треба да буде враћена са опремом, информацијама или софтвером.

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

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

Безбедност опреме корисника без надзора

Корисници 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.

Обавезе запослених подразумевају следеће:

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

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, правно лице за информационо технолошке послове обавља следеће активности:
а) инсталацију и конфигурацију система;
б) поступа у случају грешке или у других ванредних ситуација које могу да настану у току извршавања посла;
в) утврђује листу контаката за подршку у случају неочекиваних оперативних или техничких потешкоћа;
г) поновно покретање система и опоравак у случају отказа система;
д) надгледа систем.

Управљање расположивим капацитетима

Коришћење ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе система. Периодично се спроводе слеће активности:
а) брисање застарелих података;
б) повлачење из употребе апликација, система, база података или окружења.

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 информационе безбедности, као и на одговарајућим контролама приступа систему и управљању захтеваним и потребним променама.

Поступак контроле и предузимање мера против злонамерног софтвера

Дирекција у сарадњи са правним лицем за информационо технолошке послове и уз подршку Канцеларије за ИТ и е Управу одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Заштита од злонамерног софтвера подразумева:

1. формалну забрану коришћења неауторизованих софтвера;
2. имплементацију контрола које спречавају или откривају коришћење неовлашћеног софтвера;
3. успостављање формалне политике ради заштите од ризика повезаних са добијањем датотека и софтвера од или преко спољних мрежа, или на било ком другом медијуму, указујући на то које заштитне мере треба предузети;
4. смањење рањивости које може да експлоатише непријатељски софтвер, нпр. кроз управљање техничким рањивостима;
5. спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе;
6. инсталирање и редовно ажурирање софтвера за откривање злонамерног софтвера и опоравак ради претраживања рачунара и медијума као контролу из предострожности, или на рутинској основи.

Листа провера које се спроводе:
а) провера, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер;
б) провера, пре коришћења, садржаја прилога електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер; ову проверу треба спроводити на разним местима, нпр. на серверима за електронску пошту, на стоним рачунарима или приликом уласка у мрежу оператора ИКТ система;
в) проверу постојања злонамерних софтвера на веб-страницама;
г) имплементацију процедура за верификовање информација о злонамерним софтверима и

обезбеђење да су упозоравајући извештаји тачни и информативни;
д) сви корисници треба да буду свесни проблема појаве духовитих или злонамерних обмана и онога што треба да раде после њиховог пријема.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави правном лицу за информационо технолошке послове.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета Одељење за регулисање железничког тржишта, лиценце, права путника и заједничке послове у сарадњи са правним лицем за информационо технолошке послове може укинути приступ.

Заштита од губитка података

Члан 21.

Заштита од губитка оперативних података обезбеђена је обавезом чувања и архивирања документације у папирном формату.

Изузети од става 1 су подаци који се чувају у бази података на серверу Дирекције који се налази у сервер сали УЗЗПРО уз поштовање свих безбедносних мера.

Резервне копије информација и података

Резервне копије информација и радног материјала постоје у папирној форми, а по потреби запослени врше бекап података на екстерне хард дискове.

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

Члан 22.

Записивање догађаја

Податке о догађајима на мрежи органа државне управе региструје Канцеларија за ИТ и е Управу. Правно лице за информационо технолошке послове прави записе о догађајима у вези са информационом безбедношћу на радним станицама запослених.

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.

Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

Правно лице за информационе технолошке послове инсталира софтвере и

оперативне системе које за државне органе обезбеђује Канцеларија за ИТ е Управу.

Инсталацију и подешавање софтвера може да врши само правно лице за информационо технолошке послове.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

Дирекција у сарадњи са правним лицем за информационо технолошке послове 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

Дирекција у сарадњи са правним лицем за информационо технолошке послове благовремено прикупља информације о техничким рањивостима информационих система који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимањем у обзир припадајућих ризика.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, правно лице за инфомационо технолошке послове је дужно 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 ризицима.

Правно лице за информационо технолошке послове искључиво је задужено за инсталирање софтвера, водећи рачуна о свим безбедносим ризицима.

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

Члан 25.

У случају потребе спровођења ревизије ИКТ система, Дирекција ће обезбедити да ревизија има што мањи утицај на фукционисање система.

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.

Мрежне услуге укључују механизме безбедности, обезбеђивање прикључака, услуге на мрежи државних органа, као и решења за управљање безбедношћу (заштита и системи за откривање упада).

Дирекција све ове послове поверава Канцеларији за ИТ и е Управу као

администратору мреже државних органа.

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

Члан 27.

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

Правила коришћења електронске поште, Интернета и информационих ресурса

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

Приступ садржајима на Интернету је дозвољен искључиво за пословне намене.

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

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

Размена електронских порука

У Дирекцији је дозвољена размена електронских порука искључиво путем електронске поште.

Клаузула о поверљивости или неоткривању

Уговор између Дирекције и правног лица за информационо технолошке послове обавезно садржи клаузулу о поверљивости или неоткривању, у циљу заштите информација Дирекције и обавезују потписнике да информације штите и користе 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, Дирекција је дужна да обезбеди информациону безбедност у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и

рационалнијих решења.

Правно лице за информационо технолошке послове је задужено за технички надзор над реализацијом од стране извођача, односно испоручиоца.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система правно лице за информационо технолошке послове у сарадњи за Одељењем за регулисање железничког тржишта, лиценце, права путника и заједничке послове води документацију.

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 упоредила актуелна и очекивана понашања.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера.

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

За потребе тестирања ИКТ система односно делова система правно лице за информацоно технолошке послове може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

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 Дирекције морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

Пружаоци услуга имају право на приступ информацијама које су неопходне за пружање предметне услуге која је уговорена са Дирекцијом.

Дирекција успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга:

- идентификовање и документовање врсте пружаоца услуга којима ће Дирекција дозволити приступ информацијама;

- стандардизовани процес за управљање односима између пружаоца услуга;
- 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.

Уговарање 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 се достављене или на други начин учињене доступним информације и подаци могу користити искључиво на начин претходно одобрен од стране Дирекције, а 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 накнаду штете у корист Дирекције у случају повреде ове одредбе.

Пружаоци услуга дужни су да захтеве Дирекције у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе.

Одељење за регулисање железничког тржишта, лиценце, права путника и заједничке послове је одговорно за контролу приступа и надзор над извршењем уговорених обавеза.

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, Дирекција успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга

Одељење за регулисање железничког тржишта лиценце, права путника и заједничке послове редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

1. надгледање и преиспитивање услуга се може вршити преко трећег лица;

2. 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;
3. врши се оцена квалитета извршења и саобразности уговорене услуге;
4. пружалац услуге има уговорну обавезу да организује и припреми периодичне састанаке који ће обезбедити редовно извештавање. Дирекција ће унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;
5. Одељење за регулисање железничког тржишта, лиценце, права путника и заједничке послове 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, које процесуира или којима управља;

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене, утврдити поступак извештавања, праћења и поступања у складу са захтевима Дирекције 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 начин и обим извршења, у складу са утврђеним стварним потребама Дирекције.

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 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 Дирекција 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

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени је дужан да о томе одмах обавести правно лице за информационо

технолошке послове, и то на следећи начин:

1. запослени који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и послати га правном лицу за информационо технолошке послове путем електронске поште или телефоном;
2. правно лице за информациону технолошке послове врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури.

Извештавање о догађајима у вези са безбедношћу информација

Сви запослени морају бити упознати са обавезом извештавања о догађајима у вези са информационом безбедношћу.

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

Када је идетификован инцидент запослени је дужан да одмах обавести правно лице за информационо технолошке послове које затим предузима мере у циљу заштите ресурса ИКТ система.

Правно лице за информационо технолошке послове 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 правно лице за информационо технолошке послове, у што краћем року, како би се инциденти нарушавања информационе безбедности спречили и како би се спречио настанак штете.

Одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности, поступа у складу са одговарајућом процедуром.

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

Одговор на инциденте нарушавања информационе безбедности

Дирекција по потреби 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.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

Дирекција у циљу обезбеђивања континуитета обављања посла у ванредним околностима врши константну проверу и надзор ИКТ система како би се предупредиле све нежељене ситуације и како би у ванредним околностима ИКТ систем у што краћем року

био у функционалном стању.

ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Дирекције

Члан 34.

Обавеза Дирекције 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 овлашћења и одговорности у ИКТ систему Дирекције за железнице.

Ступање на снагу Акта о безбедности

Члан 35.

Овај Акт о безбедности ступа на снагу даном објављивања на огласној табли Дирекције.

В. д. директора

Лазар Мосуровић