„Инфраструктура железнице Србије“ а.д.
Број: 4/2018-644-183
Датум: 26.04.2018. године
Б е о г р а д

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, бр. 6/16 и 94/17), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС”, број 94/16) и члана 24. Статута Акционарског друштва за управљање јавном железничком инфраструктуром „Инфраструктура железнице Србије“, Београд („Службени гласник РС“, бр. 60/15, 73/15 и „Службени гласник Железнице Србије“, број 14/17), Одбор директора „Инфраструктура железнице Србије“ а.д. је, на седници одржаној дана 26.04.2018. године, донео

О Д Л У К У

1. Доноси се Акт о безбедности информационо-комуникационог система „Инфраструктура железнице Србије“ а.д.

2. Акт из тачке 1. саставни је део ове одлуке.

3. Одлука ступа на снагу даном доношења.

4. Одлуку објавити у „Службеном гласнику Железнице Србије“.

ПРЕДСЕДНИК
ОДБОРА ДИРЕКТОРА

Др Мирољуб Јевтић

„Инфраструктура железнице Србије“ а.д.
Број: 4/2018-644-183
Датум: 26.04.2018. године
Б е о г р а д

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, бр. 6/16 и 94/17), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС”, број 94/16) и члана 24. Статута Акционарског друштва за управљање јавном железничком инфраструктуром „Инфраструктура железнице Србије“, Београд („Службени гласник РС“, бр. 60/15, 73/15 и „Службени гласник Железнице Србије“, број 14/17), Одбор директора „Инфраструктура железнице Србије“ а.д. је, на седници одржаној дана 26.04.2018. године, донео

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА „ИНФРАСТРУКТУРА ЖЕЛЕЗНИЦЕ СРБИЈЕ“ А.Д.

I. ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

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

Значење израза

Члан 2.

Поједини термини употребљени у овом Акту имају следеће значење:

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

(1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;

(2) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;

(3) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

(4) организациону структуру путем које се управља ИК системом;

2) *оператор ИК система* је правно лице, орган јавне власти или организациона јединица органа јавне власти који користи ИК систем у оквиру обављања своје делатности, односно послова из своје надлежности;
3) *информациона безбедност* представља скуп мера које омогућавају да подаци којима се рукује путем ИК система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;
4) тајност је својство које значи да податак није доступан неовлашћеним лицима;
5) *интегритет* значи очуваност изворног садржаја и комплетности податка;
6) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
7) *аутентичност* је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
8) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
9) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИК система;
10) *управљање ризиком је* систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
11*) инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
12) *мере заштите ИК* система су техничке и организационе мере за управљање безбедносним ризицима ИК система;
13) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
14) *ИК систем* за рад са тајним подацима је ИК систем који је у складу са законом одређен за рад са тајним подацима;
15) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
16) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
17) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;
18) *криптоматеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
19) информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и слично.

Циљеви Акта о безбедности

Члан 3.

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 ИК система;
4) прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИК система;
5) свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Акта о безбедности

Члан 4.

Мере заштите ИК 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 Друштву морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са његовим одредбама, као и другим интерним процедурама које регулишу информациону безбедност.

Сектор за информационе технологије (у даљем тексту: Сектор за ИТ) је одговоран за спровођење и праћење примене мера безбедности, као и за проверу адекватне заштите ИК система и података на начин који је утврђен овим Актом.

Одговорност запослених

Члан 5.

Запослени у Друштву су дужни да приступају информацијама и ресурсима ИК система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

Непоштовање одредби Акта о безбедности, као и свако угрожавање или нарушавање информационе безбедности, представља повреду радне обавезе из члана 179. став 2. тачка 5) Закона о раду.

Предмет заштите

Члан 6.

Мере заштите ИК система односе се на:
- комуникациону рачунарску мрежу
- персоналне мобилне и фиксне рачунаре
- серверске системе за чување података
- апликације везане за пословање
- корисничке налоге на пословном директоријуму
- организациону структуру Друштва
- податке о пословању на централном рачунарском систему IBM
- електронску документацију
- унутрашње опште акте и процедуре

Корисницима система, који су одговорни за функционисање процеса рада, омогућен је несметан и сталан приступ подацима, који су креирани коришћењем информационо-комуникационих технологија (ИК) Друштва, а у складу са овлашћењима за одређено радно место и важећом орагнизационом структуром Друштва, или одобрењем од стране непосредног руководиоца, а уз сагласност представника Сектора за ИТ.

Својинска и ауторска права над подацима који су креирани коришћењем ИК Друштва од стране запослених у Друштву у радно време, за које су крајњи корисници плаћени од стране Друштва, припадају Друштву. Запослени Друштва са собом носе права и обавезе, посебно у погледу тачности, ажурности и доступности тих података, као и чувања пословне тајне и заштите интереса Друштва.

Пословодство Друштва је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим Актом.

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

Друштво, у циљу 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 над целокупним ИК системом, у континуитету и у складу са нормама безбедности;
- штити информације и податке на једнак начин у свим организационим јединицама;
- координира безбедност и заштиту ИК система и података у информационом систему са физичком заштитом истих.

II. МЕРЕ ЗАШТИТЕ

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

Члан 7.

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. Друштво у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

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

- Акт о организацији и систематизацији послова
- Уговори о раду

Генерални директор је дужан да донесе појединачни акт, у складу са актом о систематизацији, којим одређује одговорна лица за обезбеђивање и праћење безбедности

информационог система Друштва. Сви запослени морају бити упознати са процедуром заштите безбедности ИК система.

Друштво преко Акта о приступу Интранет мрежи утврђује начин доделе овлашћења за приступ ИК систему, степен обуке и квалификацију запослених, начин одобравања приступа запосленима од стране руководиоца, односно непосредно надређеног лица. Актом о приступу Интранет мрежи Друштва, утврђује се и одговорност сваког запосленог и одговорног лица и прописује одговорност, у случају непоштовања одредби које уређују информациону безбедност.

Коришћење ИК система је намењено пословним потребама Друштва. Носиоци ИК функције гарантују тајност садржаја информација, података и докумената у електронској форми која се прослеђује и/или складишти од стране крајњих корисника ИК система и Друштва уопште, преко електронске поште, процеса за пренос и обраду података, и помоћних програма.

Корисницима је неопходно ограничити приступ ИК систему, подацима и средствима за обраду података у складу са степеном тајности података. Крајњим корисницима ИК система је дозвољен приступ само радним станицама, мрежи и мрежним услугама за коју имају овлашћења да користе у складу са радним местом и припадајућим радним процесом.

Скуп апликација и софтвера којима располаже крајњи корисник ИК система Друштва, је дефинисан конкретним радним местом на које је запослени Друштва распоређен и радним задацима који су му додељени, а у складу са надлежностима утврђеним организационом структуром Друштва. Променом радног места и задатака, мења се и група расположивих софтвера. Коришћење ИК система за личне или приватне потребе запослених (e-mail, office алати) дозвољено је у мери у којој то коришћење не угрожава или не нарушава пословање Друштва и не крши обавезе запослених, а уз потпуну одговорност запосленог за све последице таквог коришћења ИК сиситема. Друштво искључује било какву обавезу и одговорност за коришћење ИК система за личне или приватне потребе запослених или трећих лица.

Корисници ИК система дужни су да поштују поверљивост ИК система Друштва, као и сервиса других лица у и/или изван Друштва.

Запосленима и другим корисницима ИК Друштва забрањује се да се баве:

- надгледањем или пресретањем фајлова или електронских комуникација запослених или трећих лица
- "хакерисањем" или неовлашћеним приступањем системима и/или налозима за које немају одобрење за употребу
- коришћењем туђих налога, лозинки или средстава за приступ ИК систему
- тестирањем или надгледањем рачунарских и/или мрежних безбедносних мера и "пробијањем" заштите и безбедносног система Друштва
- уношењем злонамерног кода и софтвера у информациони систем

Крајњим корисницима ИК система Друштва забрањује се да на радне станице и рачунарску мрежу и опрему Друштва самовољно прикључују било какве додатне уређаје и хардверске модуле и уређаје без одобрења носиоца ИК функције. Електронске

поруке или други електронски подаци, који покушавају да сакрију идентитет пошиљаоца, или да представе пошиљаоца као неког другог корисника, нису дозвољени.

У циљу провере функционалности ИК система и унапређења безбедности и заштите ИК система, дозвољава се надгледање, контрола рада крајњих корисника и радњи у функцији одржавања нивоа безбедности, само овлашћеним администраторима Сектора за ИТ у Друштву. У случају откривања злоупотребе коришћења ИК система, угрожавања безбедности података функционисања ИК система, носилац ИК функције је овлашћен да без упозорења делимично или потпуно, привремено или трајно искључи са рачунарске мреже Друштва сваку радну станицу или информацино-комуникациони ресурс, или да онемогући приступ ИК систему кориснику, за кога се утврди, или се сумња да се преко њега врши злоупореба, или да постоји опасност за податке, или функционисања ИК система.

У случају доказаног нарушавања безбедности ИК система и поверљивих информација или уколико корисник ИК система злоупотребљава овлашћења у коришћењу ИК система и не понаша се у складу са одредбама овог Акта и другим општим актима Друштва или на други начин изврши повреду правила и безбедносне политике Друштва, против одговорних лица биће спроведен поступак утврђивања повреде радне обавезе, у складу са одредбама Закона о раду.

Поступак утврђивања повреде радне обавезе се покреће по предлогу надлежног овлашћеног лица. Мера за повреду радне обавезе изриче се у складу са причињеном штетом, нарушеном безбедношћу и ризиком коме су ИК систем и подаци били изложени.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 8.

Друштво 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.

Радни однос или ангажовање запослених лица за обављање послова ван просторија послодавца обухвата:

- Рад на даљину
- Рад од куће

Предметно ангажовање и омогућавање обављања задатих и неопходних послова се уређује путем Процедуре за VPN приступ информационом систему (у даљем тексту: VPN процедура). VPN процедура дефинише правила и услове за повезивање на мрежу Друштва са удаљене локације. Правилном применом утврђеног поступка и начина приступа, Друштво своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи.

VPN процедура се примењује на све запослене у Друштву и сараднике који користе рачунаре или мобилне уређаје за повезивање на мрежу Друштва и уређује приступ са удаљених локација у сврху обављања посла у име и за рачун Друштва, укључујући

коришћење електронске поште и мрежних ресурса, као и начин приступа мрежи Друштва са удаљених локација.

Ауторизованим корисницима није дозвољено да користе мрежу Друштва за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада појединачно запосленог.

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 Друштва, 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 Друштва.
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. Уколико је потребно да се подаци чувају на мобилним уређајима неопходно је дефинисати потпуну енкрипцију диска преко Microsoft Bit Locker-a са чувањем лозинке код администратора рачунарске мреже.

Рад на даљину одобрава одговорно лице у Сектору за ИТ.

Коришћење мобилних уређаја

Члан 9.

Мобилни уређаји подразумевају све преносне електронске уређаје намењене за комуникацију на даљину. У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони, PDA и сви други мобилни уређаји који садржи податке и имају могућност повезивања на мрежу. Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Процедура за коришћење мобилних уређаја у Интранет мрежи Друштва дефинише начин физичке заштитите од крађе и активности које је неопходно предузети у случају крађе или губитка мобилних уређаја како не би била нарушена безбедност.
Друштво спроводи обуку запослених који користе мобилне уређаје, у циљу подизања свести о додатним ризицима до којих долази услед оваквог начина рада.

Процедуром о коришћењу мобилних уређаја потребно је установити следећа правила:

1. Сви уређаји морају бити заштићени јаком шифром. Шифра мора бити у складу са шифром на пословном директоријуму.
2. Мора бити инсталирана антивирусна заштита. Антивирусна заштита мора бити надгледана са централног портала на Интернету за антивирусни програм.

3. Мора бити усвојена и оперативна процедура за потпуно брисање података када престаје потреба за чувањем истих.
4. Крађа или губитак мобилног уређаја се мора без одлагања пријавити надлежној организационој јединици за информационе технологије и одговорном лицу, који затим спроводе активности у смислу очувања безбедности. Уколико се уређај пронађе, потребно је предати исти одговорним лицима.
5. Корисницима није дозвољено да врше измене на хардверу или инсталираном софтверу који је власништво Друштва.
6. У циљу заштите података организациона јединица за информационе технологије ће евидентирати коришћење мобилних уређаја у одговарајућим логовима, које ће у случају потребе користити за истраживања и утврђивања евентуалних злоупотреба.

Процедура се примењује на све стално запослене, запослене на одређено време или лица ангажована по другим основима, који имају приступ или користе мобилне уређаје у власништву Друштва.

Право на коришћење мобилних уређаја ван седишта Друштва се стиче на основу писаног захтева корисника мобилног уређаја упућеног Сектору за ИТ, односно одговорном лицу. Мобилни уређаји који се користе морају бити претходно одобрени и/или набављени од стране Друштва, и оцењени као компатибилни са захтевима обезбеђивања адекватног степена заштите.

Рад на даљину може се остварити и коришћењем уређаја који нису мобилни (на пример, десктоп рачунари). Ови уређаји, при томе, 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. Подешавање ових уређаја врше запослени у Сектору за ИТ. Корисници ових уређаја морају обезбедити довољно безбедан простор за њихов рад (засебна соба, положај дисплеја такав да се онемогући посматрање од стране неовлашћених особа и слично).

Одговорно лице у Сектору за ИТ води евиденцију о свим уређајима намењеним за рад на даљину. Евиденција о уређајима треба да садржи податке који су неопходни да би се уређај и/или корисник недвосмислено идентификовали, као што су произвођач, модел, серијски број, инвентарски број, MAC адреса, IMSI, IMEI, корисник који је задужио уређај и његов јединствени матични број и слично.

Корисник мобилног уређаја у обавези је да крађу или губитак мобилног уређаја пријави Сектору за ИТ без одлагања, а у року од 12 сати да достави писану изјаву о околностима губитка или крађе мобилног уређаја. Одговорно лице у Сектору за ИТ је у обавези да, по пријави крађе или губитка мобилног уређаја, неодложно блокира несталом мобилном уређају приступ информационом систему и кориснику промени креденцијале за приступ. У случају да се пронађе мобилни уређај чији нестанак је пријављен, Одговорно лице у Сектору за ИТ извршиће преглед уређаја и утврдити да ли он може бити поново коришћен за рад на даљину или не.

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

Члан 10.

Друштво се стара да запослени који управљају ИК системом, односно запослени који користе ИК систем имају адекватан степен образовања и стручну способност, као и свест о значају послова које обављају. Њихова одговорност је утврђена Уговором о раду или ангажовању на привременим и повременим пословима.

Провера кандидата и услови запошљавања

Друштво не спроводи проверу знања у циљу провере испуњености услова сваког појединачног кандидата за рад.

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

Пословодство Друштва је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим Актом и важећим процедурама.

У циљу развоја, имплементације и одржавања система заштите и безбедности података, Друштво 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

Запослени Сектора за ИТ континуирано се обучавају у циљу унапређења техничког и технолошког знања. Ова лица су ауторизована 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

Администратори рачунарске мреже у Друштву 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.

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

Члан 11.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИК 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:

- Процедуром о правима приступа информационом систему
- Уговором о раду
- Споразумом о поверљивости

За поступања приликом престанка запослења или ангажовања задужен/а је Сектор за људске ресурсе и опште послове и Сектор за ИТ, који предузимају следеће активности:

- провера испуњености свих услова у погледу чувања и изношења података у електронском и папирном формату,
- преглед свих налога и приступа систему који су били доступни запосленом,
- преузимање од запосленог електронске и друге мобилне уређаје,
- утврђивање начина контакта са бившим запосленим након одласка,
- провера враћених мобилних уређаја и уређаја за преношење података,
- давање налога за укидање налога електронске поште и свих других права приступа систему Друштва на дан престанка радног односа или другог основа ангажовања бившег запосленог,
- преглед свих налога за приступ одлазећег запосленог и прикупљање приступне шифре и кодова са циљем укидања/промене истих на дан одласка,
- преузимање картице или других уређаја којима се омогућава приступ пословним просторијама и опреми Друштва.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 12.

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

Пописивање имовине

Друштво 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. Друштво прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Евиденцију о информационим добрима води Сектор за ИТ.

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.

Друштво у оквиру интерног акта о руковању имовином уређује правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација.

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

Током отказног рока запослених, Друштво контролише 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 13.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем за Друштво.

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

Друштво 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 или угрожава опстанак.

Друштво 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 података у покрету ради боље и интелигентније интеграције са DLP, WEB gateway и осталим производима за заштиту параметара и крајњих уређаја;
- Заштите садржаја;
- Интеграције са системима за архивирање.

Заштита носача података

Члан 14.

Друштво спроводи процедуре спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, води Сектор за ИТ.

Управљање преносним носачима података

Друштво је дужно да за управљање преносним носачима података развија и имплементира процедуру о управљању преносним носачима, у складу са усвојеном Шемом класификовања података из члана 13. овог акта.

Крајњи корисник ИК система дужан је да поштује мере безбедног коришћења носача података, а у складу са овим актом.

Корисник ИК система је одговоран за употребу носача података, у складу са следећим:

- неопходно је све носаче података и преносне медије, приликом повезивања на матични рачунар скенирати званичним Антивирус програмом;
- 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;
- спречити неовлашћено модификовање, уклањање или уништење података, информација и садржаја неопходних за рад Друштва, а који се чувају на носачима података.
- носаче података који садрже информације треба штитити од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта.
- све осетљиве и поверљиве информације у електронском облику запослени морају одложити на сигурно место ван домашаја неовлашћених лица на крају радног дана или када нису присутни на свом радном месту.

Расходовање носача података

Када више нису потребни, медијуми се расходују на безбедан начин, применом Процедуре за безбедносно расходовање медијума.

Друштво врши безбедносно расходовање медијума и свођење на минимум ризика од доласка осетљивих информација до неовлашћених особа.

Процедура за безбедносно расходовање медијума који садрже поверљиве информације разликује раличите начине процеса расходовања, који су сразмерни осетљивости тих информација.

Процедура за безбедносно расходовање медијума:

- медијуме који садрже осетљиве информације треба расходовати у складу са Законом

- неопходно је уредити начин за идентификовање ставки за које ће можда бити потребно безбедносно расходовање;
- расходовање осетљивих елемената је потребно евидентирати, како би се сачувао траг за проверу.

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.

У случају транспорта медија са подацима, Сектор за ИТ одређује лице које ће вршити транспорт и начин транспорта.

Ограничење приступа подацима и средствима за обраду података

Члан 15.

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.

Друштво ће формирати Контролну листу приступа која садржи попис свих информационих објеката и субјекте који им могу приступити.

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

Друштво ће посебним документом уредити приступ мрежи и мрежним уређајима.

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

Члан 16.

Друштво управља приступом ИК систему и услугама кроз употребу корисничких идентификатора. Управљање корисничким идентификаторима врши се поштујући следеће принципе:

- кориснички идентификатори (Username и Password) 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;
- коришћење заједничких идентификатора дозвољава се само онда када је то неопходно за обављање посла уз претходно одобрење надлежног сектора као и Сектора за ИТ;
- вишеструки кориснички идентификатори се периодично проверавају и уклањају или онемогућавају по потреби;

- вишеструки идентификатори неког корисника се не издају другим корисницима који немају потребе и овлашћења за коришћење.

Сваком кориснику се додељује право приступа ИК 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 Сектора за ИТ.

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

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

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

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

Друштво периодично врши провреру права корисника за 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 17.

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 увек када постоји било какав наговештај могућег компромитовања.

Облик шифре је дефинисан политиком сваког система понаособ (дужина шифре, коришћење специјалних знакова, временско трајање шифре, и сл.)

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

Члан 18.

У циљу заштите података, Друштво развија и имплементира политику коришћења криптографских контрола, и успоставља механизме и систем за управљање кључевима.

Криптозаштита обезбеђује:

- Аутентификацију (идентификацију корисника и других системских ентитета који захтевају приступ или одобрење трансакције);
- Непорецивост (примена криптографских техника, најчешће дигиталног потписа, како би се добила потврда о извршавању или неизвршавању неке трансакције од стране појединачног корисника);
- Поверљивост (применом шифровања врши се заштита осетљивих или критичних информација које се складиште или се преносе);
- Интегритет (непроменљивост података који се преносе).

Поступак криптографске контроле обухвата:

- анализу и процене потребе примене криптографије у пословним процесима укључујући опште принципе према којима би пословне информације требало да се штите;
- ниво заштите се одређује узимањем у обзир типа алгоритма за криптовање података, јачине криптографског алгоритма и квалитета криптографског алгоритма;
- примену шифровања за заштиту осетљивих података приликом преноса мобилним или другим медијумима, уређајима или преко комуникационих водова;
- управљање кључевима (заштита криптографских кључева, повраћај шифрованих података у случају губљења, компромитовања или оштећења кључева).

Управљање кључевима

Друштво тренутно не примењује методе за управљање кључевима.

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

Члан 19.

Друштво је дужно да предузме мере ради спречавања неовлашћеног физичког приступа сервер салама, у којима се налазе средства и документи ИК 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:

- Зону раздвајања представља техничка служба која ради 24 сата и одговорна је за рад сервера у сервер сали.
- Систем електронске браве који омогућава улазак у салу само овлашћеним особама.

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.

Контролу уласка предстрављају дупла враза са интерфонским системом и електронском бравом и недељним променама шифре за улазак у сервер салу.

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

Члан 20.

Постављање и заштита опреме

Опрему се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућности за неовлашћени приступ.

Безбедност опреме се обезбеђује преко:

- Постављања у одговарајуће ормане који се закључавају
- Постављања у техничке собе и сервер сале где је контролисан приступ преко алармног система и засебног кључа
- Постављања у просторије које су под надзором 24 сата дневно
- Редовне контроле рада система и промене конфигурација опреме

Одговорно лице из Сектора за ИТ, по налогу директора Сектора за ИТ, редовно прати услове околине, као што су температура и влажност, који би могли негативно да утичу на рад опреме за обраду информација.

Помоћне функције за подршку – напајање и климатизација

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;

Одржавање климатизације у исправном стању се врши:

- у складу са спецификацијама опреме произвођача и прописима;
- редовном проценом капацитета опреме и прилагођавањем у складу са потребама
- редовном контолом темпрературе и влажности у просторији

Безбедносни елементи приликом постављања каблова

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 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 просторијама 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 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

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.

- 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.
- Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана.
- 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.
- Лаптоп рачунари морају бити везани уз помоћ одговарајуће опреме или закључани у фиоци. Таблети и остали преносни уређаји морају бити закључани у фиоци.
- Носиоци података као што су дискови и flash меморија морају бити одложени и закључани.
- Шифре за приступ не смеју бити написане и остављене на приступачном месту.
- Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.
- 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 21.

Усвајање и примена радних процедура

Друштво ће усвојити радне процедуре које садрже инструкције за детаљно извршење следећих послова:

- инсталација и конфигурација система;
- обраду и поступање са информацијама (аутоматски и мануелно);

- израда резервних копија;
- захтеви за временски распоред активности;
- инструкције за поступање према грешкама или другим ванредним стањима која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција;
- контакти за подршку (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;
- инструкције за поступања према поверљивим подацима;
- процедуре за поновно покретање система и опоравак, које се користе у случају отказа система;
- управљање информацијама о трагу провере система и системским записима (логовима);
- процедуре за надгледање.

За усвајање, измене и допуне радних процедура овлашћен је директор Сектора за ИТ.

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 слеће 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.

За обезбеђивање исправног и безбедног функционисања средстава за обраду података и примену радних процедура одговоран је директор Сектора за ИТ.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 22.

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

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

Процедура заштите од злонамерног софтвера:

1) формална забрана коришћења неауторизованих софтвера;

2) имплементација контрола које спречавају или откривају коришћење неовлашћеног софтвера;
3) имплементација контрола које спречавају или откривају коришћење познатих или сумњивих компромитованих веб-сајтова;
4) 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;
5) смањење рањивости које може да експлоатише непријатељски софтвер, нпр. кроз управљање техничким рањивостима;
6) 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;
7) инсталирање и редовно ажурирање софтвера за откривање непријатеског софтвера и опоравак ради претраживања рачунара и медијума као контролу из предострожности, или на рутинској основи.

Листа провера које се спроводе:

а) проверу, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер;
б) проверу, пре коришћења, садржаја придружених порукама 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 организације;
в) проверу постојања злонамерни софтвера на веб-страницама;
г) дефинисање процедура за менаџмент и одговорности за поступање са заштитом од злонамерног софтвера у системима, обука за њихово коришћење, извештавање и опоравак од напада злонамерним софтвером;
д) припрему одговарајућих планова за континуитет пословања приликом опоравка од напада непрјатељским софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак;
ђ) имплементацију процедура за редовно прикупљање информација, као што је претплата на адресне спискове за доставу или провера веб-страница на којима се дају информације о новим злонамерним софтверима;
е) имплементацију процедура за верификовање информација о злонамерним софтверима и обезбеђење да су упозоравајући извештаји тачни и информативни; руководиоци треба да осигурају да се за разликовање лажних од стварних злонамерних софтвера користе квалификовани извори, нпр. проверени часописи, поуздане странице на интернет мрежи или испоручиоци програма против злонамерних софтвера; сви корисници треба да буду свесни проблема појаве духовитих или злонамерних обмана и онога што треба да раде после њиховог пријема.

Препоручује се доношење и процедуре о антивирусној заштити и процедуре о подизању свести запослених о информационој безбедности.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави help desku Сектора за ИТ.

У циљу заштите, односно упада у ИК систем Друштва са Интернета, одговорно лице из Сектора за ИТ, по налогу директора Сектора за ИТ, је дужно да одржава систем за спречавање упада.

Корисницима који су прикључени на ИК систем у случају доказане злоупотребе Интернета директор Сектора за ИТ може укинути приступ.

Заштита од губитка података

Члан 23.

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

Резервне копије информација 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 ИК система.

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

План израде резервних копија информација:

- тачне и потпуне записе о резервним копијама и документоване процедуре обнављања;
- обим и учесталост израде разервних копија;
- резервне копије треба да одражавају пословне потребе организације и критичност тих информација по континуитет пословања организације;
- треба их складиштити на локацији на довољној удаљености, како би се избегло свако оштећење на главној локацији;
- резервним копијама информација треба дати одговарајући ниво физичке заштите и заштите од утицаја околине (описано у тачки 12) који је доследан мерилима која се примењују на главној локацији;
- медијуме са резервним копијама треба редовно проверавати, ради сигурности њихове употребе у ванредним ситуацијама и када је то неопходно;
- у ситуацијама у којима је важна поверљивост, резервне копије треба заштитити помоћу шифровања.

За заштиту од губитка података је одговоран је директор Сектора за ИТ.

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

Члан 24.

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

Записивање догађаја

Друштво 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.

За чување података о догађајима који могу бити од значаја за безбедност ИК система одговоран је директор Сектора за ИТ.

Обезбеђивање интегритета софтвера и оперативних система

Члан 25.

Друштво спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система у складу са смерницама за контролу промена и инсталацију софтвера.

Смернице:

- 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.

Заштита од злоупотребе техничких безбедносних слабости ИК система

Члан 26.

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

Управљање техничким рањивостима

Друштво благовремено прикупља информације о техничким рањивостима информационих система који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимањем у обзир припадајућих ризика.

Посебне информације које су потребне за подршку управљања техничким рањивостима обухватају продавца софтвера, бројеве верзија, текуће стање размештаја, као и особе које су одговорне за тај софтвер.

Смернице:

- Друштво дефинише и успоставља улоге и одговорности у вези са управљањем техничким рањивостима, укључујући надзор, оцену ризика услед утврђене рањивости, исправке, следљивост имовине и све одговорности за потребна координирања;
- најмање једном месечно а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИК система.
- дефинише се временски распоред реаговања на обавештење о могућим техничким рањивостима;
- када је могућа техничка рањивост идентификована, тада се идентификују припадајући ризици и акције које треба предузети; такве акције могу да обухвате исправке рањивих система и/или примену других контрола;
- креира се процедура која узима у обзир ситуацију у којој је идентификована рањивост, али не постоји погодна контрамера. У овој ситуацији, организација треба да процени ризик у односу на познате рањивости и дефинише одговарајуће мере за отривање, као и корективне мере.

Уколико се идентификују рањивости које могу да угрозе безбедност ИК система, одговорно лице из Сектора за ИТ, по налогу директора Сектора за ИТ, 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 ИК система безбедносним слабостима.

Инсталирање софтвера на радним станицама раде искључиво администратори уз предходно писмено одобрење.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 27.

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.

Одговорно лице из Сектора за ИТ, по налогу директора Сектора за ИТ је дужно да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

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

Члан 28.

Заштита података који се преносе комуникационим средствима унутар Друштва, између оператора ИК система и лица ван оператора ИК 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 намену коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

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

Члан 29.

Извештавање о догађајима у вези са безбедношћу информација

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

Директор Сектора за ИТ је у дужан да припреми план и неколико метода комуникације које би могле да се примене у зависности од инцидента. Могуће методе комуникације су: електорнска пошта, 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.

Процедура:

1. Запослени који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и послати га електронском поштом Сектору за ИТ (help desk)/ позвати број/ пријавити проблем путем Интернет стране за help desk);
2. Адресу електронске поште, број телефона и Интернет страну за help desk проверава систем администратор;
3. Систем администратор врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури.

Када је индетификован инцидент, запослени је дужан да одмах обавести директора Сектора за ИТ, и предузме мере у циљу заштите ресурса ИК система.

Одговорно лице из Сектора за ИТ, по налогу директора Сектора за ИТ 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 ИК система директора Сектора за ИТ 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 ИК 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

Друштво је у обавези да усвоји План за превенцију безбедносних ризика.

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

Прикупљање доказа

Друштво дефинише и примењује процедуре за идентификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају утврђивања одговорности запосленог за повреду радне обавезе.

III. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Друштва

Члан 30.

Друштво има обавезу да најмање једном годишње изврши проверу ИК система и изврши евентуалне измене Правилника о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИК систему Друштва.

Ступање на снагу Акта о безбедности

Члан 31.

Овај Акт о безбедности ступа на снагу даном доношења и објављује се у „Службеном гласнику Железнице Србије".

ПРЕДСЕДНИК
ОДБОРА ДИРЕКТОРА

Др Мирољуб Јевтић