РЕПУБЛИКА СРБИЈА
ЗАВОД ЗА ИНТЕЛЕКТУАЛНУ СВОЈИНУ
990 Број: 012-9207/2023-01
Датум: 28.6.2023. године
Кнегиње Љубице 5, Београд

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС", број 6/16, 94/17 и 77/19), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС", број 94/16), на основу члана 35. став 1. Закона о државној управи („Службени гласник РС", бр. 79/05, 101/07, 95/10, 99/14, 47/18 и 30/18-др. Закон), директор Завода за интелектуалну својину доноси

Правилник о безбедности информационо-комуникационог система Завода за интелектуалну својину

I. Уводне одредбе

Члан 1.

Овим Правилником, у складу са Законом о информационој безбедности („Службени гласник РС", број 6/16, 94/17 и 77/19) и Уредбом 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), утврђују се мере и заштите, а нарочито принципи, начин процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информационо-комуникационих система (у даљем тексту ИКТ систем).

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.

Члан 3.

Овај Правилник је обавезујући за све унутрашње организационе јединице Завода за интелектуалну својину и за све кориснике информатичких ресурса, као и за трећа лица која користе информатичке ресурсе Завода.

Непоштовање одредби овог Правилника, као и свако угрожавање или нарушавање информационе безбедности повлачи дисциплинску одговорност запосленог - корисника информатичких ресурса.

Шеф Одсека за информациони систем и запослени у Одсеку 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.

Члан 4.

Поједини изрази употребљени у овом правилнику имају следеће значење:

1) *информационо-комуникациони систем (ИКТ систем)* је технолошко - организациона целина која обухвата све уређаје за електронску обраду података (хардверске и софтверске *компоненте*, мрежу и мрежне ресурсе, сервер и осталу комуникациону опрему);

2) *оператер ИКТ система* је Завод за интелектуалну својину, као посебна организација у систему државне управе тј. државни орган;

3) *информациона безбедност* је скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

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

5) *интегритет* значи очуваност изворног садржаја и комплетности податка;

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

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

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

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

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

11) *инцидент* је унутрашња или спољна околност или догађај којим се угрожава или

нарушава информациона безбедност;

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

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

14) *информациона добра* обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике, процедуре и слично;

15) *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

16) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

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

18) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;

19) *криптоматеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

20) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

21) *ВПН (Virtual Private Network)* је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;

22) *МАК адреса (Media Access Control Address)* је јединствен број, којим се врши идентификација уређаја на мрежи;

23) *Бекап* је резервна копија података;

24) Архива је збирка података који се чува у складу са прописима о архивирању;

25) *Преузимање (download)* је трансфер података са централног рачунара или web презентације на локални рачунар;

26) *УПС (Uninterruptible Power Supply)* је уређај за непрекидно напајање електричном енергијом;

27) Фривер (*Freeware)* је бесплатан софтвер;

28) *Opensource* софтвер отвореног кода;

29) *Firewall* је „заштитни зид" односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

29) *УСБ* или флеш меморија је спољашњи медијум за складиштење података;

30) *ЦД-РОМ (Compact disk - read only memory)* је оптички диск који се користи као медијум за складиштење података;

31) *ДВД (DVD)* је оптички диск већег капацитета који се користи као медијум за складиштење података:

32) *Сториџ системи* омогућавају складиштење великих количина података, на ефикасан и сигуран начин, са тренутном доступношћу, без обзира на тип сервера и оперативног система.

II. Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Завода, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у Заводу

Члан 6.

Сваки запослени корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система, које користи ради обављања послова из своје надлежности.

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Завода, надлежан је Одсек за информациони систем, односно сви запослени са администраторским овлашћењима који су задужени за одржавање информатичких ресурса у Заводу.

Члан 7.

Послови из области безбедности су:

1) послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност;
2) послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности;
3) послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Завода, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе;
4) праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу;
5) обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента, корисник информатичких ресурса дужан је да, у циљу решавања насталог безбедоносног инцидента, инцидент, без одлагања, пријави непосредном руководиоцу, који ову информацију прослеђује електронским путем Одсеку за информациони систем.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 8.

Нерегистровани корисници, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ интернету, али не и деловима мреже кроз коју се обавља службена комуникација.

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја који су у власништву Завода и који су подешени од стране запослених из Одсека за информациони систем, на основу писане сагласности шефа Одсека, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и листе MAC адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Приступ ресурсима ИКТ система Завода са удаљених локација, од стране запослених-корисника, у циљу обављања радних задатака, омогућен је путем заштићене ВПН/интернет конекције.

Запосленом-кориснику, забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима.

Запослени из Одсека за информациони систем свакодневно контролишу приступ ресурсима ИКТ система и проверавају да ли је остварен приступ са непознатих уређаја (са непознатих MAC адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава шеф Одсека за информациони систем, а та MAC адреса се уноси у "блок" листу софтвера који се користи за контролу приступа.

Приступ ресурсима ИКТ система са приватног уређаја није дозвољен, осим ако је уређај у власништву Завода оштећен и није обезбеђена замена.

Трећем лицу могу се одобрити права приступа ИКТ систему уз претходно закључење одговарајућег уговора, којим се прецизно дефинишу услови и обим права приступа, укључујући и све релевантне безбедоносне захтеве.

Изузетно од става 8. овог члана, у случају неопходних и хитних послова могу се одобрити права приступа ИКТ систему трећем лицу по усменом налогу директора Завода, односно овлашћеног лица, о чему ће се накнадно, по завршетку посла, сачинити записник о оствареном приступу.

Ако се установи повреда уговорне обавезе или прекорачење овлашћења по основу уговора, одобрени приступ се одмах укида.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води запослени из Одсека за информациони систем, а по одобрењу директора, на основу предлога шефа Одсека за информациони систем.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени - сертификовани од стране запослених из Одсека за информациони систем и могу се користити само за обављање послова у надлежности запосленог-корисника.

Запослени из Одсека за информациони систем су дужни да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава уради бекап података који се налазе у мобилном уређају, а потом их обришу из уређаја и по повратку из сервиса поново врате податке у мобилни уређај.

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

Члан 9.

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места.

Систем администратор је дужан да сваког корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Завода.

Свако коришћење ИКТ ресурса Завода од стране запосленог-корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

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

Члан 10.

У случају промене послова, односно надлежности запосленог-корисника, запослени са администраторским овлашћењима из Одсека за информациони систем, ће извршити промену привилегија које је запослени-корисник имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

У случају престанка радног ангажовања запосленог-корисника, кориснички налог се деактивира.

По престанку радног односа или радног ангажовања, као и промени радног места запосленог-корисника, непосредни руководилац је дужан да електронским путем обавести Одсек за информациони систем ради укидања, односно измене приступних привилегија тог запосленог-корисника.

Корисник ИКТ ресурса, након престанка радног ангажовања у Заводу не сме да открива податке који су од значаја за информациону безбедност ИКТ система, под претњом кривичне и материјалне одговорности.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра су сви ресурси који садрже пословне информације Завода, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе ИКТ систем и слично.

Евиденцију о информационим добрима води Одсек за информациони систем у папирној или електронској форми.

Предмет заштите обухвата:

1) хардверске и софтверске компоненте ИКТ система;
2) подаци који се обрађују или чувају на компонентама ИКТ система;
3) кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком Закона о информационој безбедности

Члан 12.

Подаци који се налазе у ИКТ систему представљају пословну тајну и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. гласник РС". бр. 53/11).

Заштита носача података

Члан 13.

Директор ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном тајности у складу са Законом о тајности података („Службени гласник РС", бр. 104/09) тако да:

1) подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени којима је издат сертификат за приступ тајним подацима;
2) подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск. УСБ, ЦД, ДВД. сториџ систем), само од стране запослених којима је издат сертификат за приступ тајним подацима, а по налогу директора.

Евиденцију носача на којима су снимљени подаци, воде запослени којима је издат сертификат за приступ тајним подацима, а по налогу директора и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, шеф Одсека за информациони систем ће одредити одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на медијима, подаци морају бити неповратно обрисани, а ако то није могуће, такви медији морају бити физички оштећени, односно уништени.

Ограничење приступа подацима и средствима за обраду података

Члан 14.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има.

Запослени-корисник који има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским, хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Запослени-корисник може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору за подешавање корисничког профила и радне станице.

Запослени-корисник који на било који начин злоупотреби корисничка права, односно ресурсе ИКТ система, подлеже кривичној, материјалној и дисциплинској одговорности.

Запослени-корисник дужан је да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система, и то да:

1) користи информатичке ресурсе искључиво у пословне сврхе;
2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Завода и да могу бити предмет надгледања и прегледања;
3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4) безбедно чува своје лозинке, односно да их не одаје другим лицима;
5) мења лозинке сагласно утврђеним правилима;
6) пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу;
7) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца, електронским путем Одсеку за информациони систем;
8) обезбеди сигурност података у складу са важећим прописима;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (backup) података у складу са прописаним процедурама;
13) користи интернет и електронску пошту у Заводу у складу са смерницама за заштиту које објављују државни органи надлежни за информациону безбедност;
14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
15) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
16) прихвати да технике сигурности (анти вирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;

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

Члан 15.

Право приступа имају само запослени – корисници који имају администраторске или корисничке налоге.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Администраторски налог може да користи искључиво запослени са администраторским овлашћењима, односно запослени у Одсеку за информациони систем коме је то овлашћење дато од стране шефа Одсека.

Кориснички налог се састоји од корисничког имена и лозинке на основу које се врши аутентификација – провера идентитета – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог – корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева руководица уже унутрашње јединице у којој је запослени-корисник запослен.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 16.

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

Сви корисници су дужни да:

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

Шифре не заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и морају садржати 8 карактера, мала и велика слова као и цифре.

Корисници су дужни да привремене шифре промене приликом првог пријављивања.

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

Члан 17.

Приступ ресурсима ИКТ система Завода не захтева посебну криптозаштиту.

Запослени-корисници користе квалификоване електронске сертификате за електронско потписивање докумената, као и аутентификацију и ауторизацију приступа појединим апликацијама.

Запослени на пословима ИКТ задужени су за инсталацију потребног софтвера и хардвера за коришћење сертификата.

Запослени-корисници дужни су да чувају своје квалификоване електронске сертификате како не би дошли у посед других лица.

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

Члан 18.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује са као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном видљиво означеном простору, који је обезбеђен механичком бравом и видео надзором.

Простор мора да буде обезбеђен од пожара и других елементарних непогода и у њему треба да буде одговарајућа температура.

Евиденцију о уласку у ову зону воде запослени у Одсеку за информациони систем.

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

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

Члан 19.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система, односно запосленима из Одсека за информациони систем.

Осим администратора система и запослених на пословима одржавања ИКТ система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу шефа Одсека за инфорамциони систем и уз присуство запосленог Одсека за инфорамциони систем.

Приступ административној зони може имати и лице које обавља послове одржавања хигијене уз присуство запосленог Одсека за инфорамциони систем.

Просторија мора бити видљиво обележена и у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима.

Прозори и врата на овој просторији морају увек бити затворени. Сервери и активна мрежна опрема (switch, modem, router, firewall), морају стално бити прикључени на уређаје за непрекидно напајање - УПС.

У случају нестанка електричне енергије, у периоду дужем од капацитета УПС-а. овпашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и слично) може изнети и без одобрења шефа Одсека за информациони систем и директора Завода.

У случају изношења опреме ради селидбе или сервисирања, неопходно је одобрење шефа Одсека за информациони систем.

Ако се опрема износи ради сервисирања, потребно је сачинити и записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Завода.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 20.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим планирају, односно предлажу одређене мере шефу Одсека за информациони систем.

Пре увођења у рад новог софтвера неопходно је направити резервну копију постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију.

Инсталирање новог софтвера као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запослених-корисника.

У случају да се на новој верзији софтвера који је уведен у оперативни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери и подаци који су намењени тестирању и развоју.

При тестирању софтвера је потребно обезбедити неометано функционисање ИКТ система. Забрањено је коришћење сервера који се користе у оперативном раду за тестирање софтвера, на начин који може да заустави нормално функционисање ИКТ система.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 21.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (УСБ меморија, ЦД итд.), инсталацијом нелиценцираног софтвера и слично.

За успешну заштиту од злонамерног софтвера на свакој радној станици је инсталиран антивирусни програм, који се аутоматски ажурира.

На захтев администратора система, запослени су дужни да оставе укључене радне станице након завршетка рада за потребе одржавања.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања радних станица или преносних медија.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером.

Ризик од евентуалног губитка података приликом чишћења медија од вируса сноси доносилац медија.

У циљу заштите, односно упада у ИКТ систем Завода са интернета, Одсек за информациони систем је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет, при чему запослени са администраторским овлашћењима из Одсека за информациони систем могу укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а свака радна станица на којој се запосленом омогућује приступ интернету мора бити одговарајуће подешена и заштићена, при чему подешавања врше запослени са администраторским овлашћењима из Одсека за информациони систем.

Приликом коришћења интернета треба избегавати сумњиве веб странице, с обзиром да то може проузроковати проблеме - неприметно инсталирање шпијунских програма и слично.

Корисник информатичких ресурса дужан је да, без одлагања, пријави непосредном руководиоцу свако уочавање или сумњу о наступању инцидента којим се угрожава сигурност ИКТ система.

Информацију о инциденту руководилац је дужан да одмах проследи запосленима са администраторским овлашћењима у Одсеку за информациони систем.

Недозвољена употреба интернета обухвата:

1. инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
2. нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
3. намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси и друге врсте малициозних софтвера);
4. недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
5. преузимање (download) података великог обима које проузрокује оптерећење мрежне везе;
6. преузимање (download) материјала заштићених ауторским правима;
7. коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и слично);
8. недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

1. службене налоге за електронску пошту користити искључиво за службену комуникацију и пријављивање на сервисе из оквира пословног окружења (не користити за личну комуникацију, прослеђивање ланчаних порука, за пријаве на сервисе електронског

банкарства, комуналних услуга и друге приватне потребе);

2. електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;

3. забрањено је одавање података као што су нпр. корисничко име, лозинка, број телефона, алтернативна адреса електронске поште и слично.

Заштита од губитка података

Члан 22.

Завод за интелектуалну својину врши израду копија које обухватају системске информације и податке који су неопходни за опоравак система у случају наступања последица изазваних ванредним околностима.

Израда резервних копија база података се обавезно врши на преносиве медије (ЦД, ДВД, флеш диск, магнетна трака, спољни хард диск, сториџ систем), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

Израда резервних копија идентификованих фолдера, фајлова-докумената се врши најмање једном недељно, месечно и годишње.

Израда резервних копија података о запосленима-корисницима, се врши најмање једном месечно.

Израда дневних резервних копија података се врши сваки радни дан у недељи.

Израда недељних резервних копија података се врши последњег радног дана у недељи, у онолико недељних примерака колико има последњих радних дана у месецу.

Израда месечних резервних копија података се врши последњег радног дана у месецу, за сваки месец посебно.

Годишње копирање-архивирање врши се последњег радног дана у години.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе („Сл Гласник РС", бр 10/93, 14/93-исправка, 67/16, 3/17 и 20/22- др.упутство).

Сваки примерак преносног информатичког медија са копијама-архивама мора бити означен бројем, врстом (дневна, недељна, месечна, годишња), датумом израде копије-архиве, као и именом запосленог-корисника који је извршио копирање-архивирање.

Дневне, недељне, месечне и годишње копије-архиве се чувају у просторији која је обезбеђена физички и у складу са мерама заштите од пожара.

Годишње копије-архиве се израђују у два примерка, од којих се један чува у просторији у којој се чувају дневне, недељне и месечне копије-архиве а други примерак се предаје Одељењу за регистре.

Исправност копија-архива проверава се најмање на шест месеци и то тако што се изврши повраћај база података које се налазе на медију, при чему враћени подаци након повраћаја треба да буду исправни и спремни за употребу.

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

Члан 23.

О активностима администратора и запослених-корисника воде се дневници активности (*activity log, history, security log, transaction log* и друго).

Систем за контролу и дојаву о грешкама и неовлашћеним активностима мора бити подешен тако да одмах обавештава запослене са администраторским овлашћењима и шефа Одсека за информациони систем, о свим нерегуларним активностима запослених-корисника, о покушајима упада и упадима у систем.

Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

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

Смернице за контролу промена и инсталацију софтвера:

1. ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљени администратори, по добијању одговарајућег овлашћења од руководиоца;
2. оперативни системи треба да садрже само одобрене извршне кодове, а не и развојне кодове или компилаторе;
3. 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;
4. треба осигурати да су све одговарајуће библиотеке изворних програма ажуриране;
5. пре имплементације било каквих промена, треба успоставити стратегију повратка на претходно стање;
6. као меру предострожности за неочекиване ситуације треба сачувати претходне верзије апликативног софтвера.

Инсталацију и подешавање софтвера може само да врши запослени са администраторским овлашћењима у Одсеку за информациони систем, односно запослени који има овлашћење за то.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера.

Пре сваке инсталације нове верзије софтвера, односно подешавања, неопходно је направити копију постојећег, како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

Запослени са администраторским овлашћењима у Одсеку за информациони систем, најмање једном месечно, а по потреби и чешће, 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.

Запослени са администраторским овлашћењима у Одсеку за информациони систем 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.

За софтверске и друге технологије (засноване на списку имовине) се одређују информациони ресурси за идентификовање одговарајућих техничких рањивости и за одржавање свести о истима, ови информациони ресурси се ажурирају на основу измена у инвентару или онда када се идентификују нови или други корисни ресурси.

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. У зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, предузете активности се спроводе у складу са контролама које су везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности. Ако је исправка доступна од легитимног извора, онда се оцењују ризици у вези са инсталирањем те исправке (ризике који настају услед рањивости треба упоредити са ризиком везаним за инсталирање исправке).

Исправке се морају прво испробати и вредновати пре него што се трајно угради, како би се осигурало да ће оне бити ефективне и да неће довести до споредних утицаја који се не могу толерисати; ако исправка није на располагању, онда треба размотрити друге контроле, као што су деактивирање услуга или могућности које се односе на рањивост, прилагођавање или додавање контрола приступа или појачано надгледање како би се открили или спречили постојећи напади и утицало на повећање свести о рањивости.

О свим предузетим процедурама се праве записи за проверу, а процес управљања техничким рањивостима треба редовно надгледати и вредновати како би се осигурале његова ефективност и ефикасност.

Најпре се узимају у разматрање системи са високим ризиком. Ефективан процес управљања техничким рањивостима се усклађује са активностима које се односе на управљање инцидентима, тако да обезбеди техничке процедуре које треба спровести ако се догоди неки инцидент.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, запослени са администраторским налогом у Одсеку за информациони систем, дужан да у најкраћем року изврши подешавања, односно инсталира софтвер који ће отклонити уочене рањивости.

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

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

Члан 26.

Приликом спровођења ревизије ИКТ система, запослени са администраторским налогом у Одсеку за информациони систем, обезбеђује да ревизија има што мањи утицај на фукционисање система.

Уколико то није могуће у радно време, онда се врши након завршетка радног времена запослених-корисника, чији би пословни процес био ометан, уз претходну сагласност непосредног руководиоца запосленог-корисника.

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.

Спецификација мрежних услуга, било да се оне пружају унутар самог Завода било од стране трећих лица, укључују механизме безбедности, врсте услуга утврђених на захтев руководства.

Мрежне услуге обухватају обезбеђивање прикључака, услуге на приватним мрежама и мрежама са додатним функцијама, као и решења за управљање безбедношћу (заштита и системи за откривање упада).

У мрежама су међусобно раздвојене групе информационих услуга, корисника и система, а запослени са администраторским налогом у Одсеку за информациони систем је одговоран за управљање мрежом.

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

Члан 28.

Заштита података који се преносе комуникационим средствима унутар Завода, као и размена података са државним органима, органима локалних самоуправа, правним и физичким лицима, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

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

Члан 29.

Начин инсталације нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Заводу биће дефинисан уговором који ће бити склопљен са тим лицима.

Запослени из Одсека за информациони систем су задужени за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система запослени из Одсека за информациони систем воде документацију.

Документација из претходног става мора да садржи описе свих процедура, а посебно процедура које се односе на безбедност ИКТ система.

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

Члан 30.

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

Приликом тестирања система, подаци који су означени ознаком тајности, односно поверљивости или представљају податке о личности, запослени из Одсека за информациони система одговарају за податке у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 31.

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

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

Запослени из Одсека за информациони система су одговорни за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

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

Члан 32.

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

Запослени са администраторским овлашћењима у Одсеку за информациони систем, 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 Завода и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;
5. запослени са администраторским овлашћењима у Одсеку за информациони систем, 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;
6. запослени са администраторским овлашћењима у Одсеку за информациони систем одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања;

7. преиспитује трагове провере и записа о догађајима у вези са безбедношћу код пружаоца услуга, односно оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.

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

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

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.

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 Завод 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 33.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени је дужан да одмах, без одлагања обавести непосредног руководиоца.

По пријему пријаве, информацију о инциденту руководилац је дужан да исту одмах проследи запосленима са администраторским овлашћењима у Одсеку за информациони систем како би се одмах предузеле мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, („Сл. гласник РС", бр. 11/20), шеф Одсека за информациони систем дужан је да поред директора Завода обавести и надлежни орган дефинисан наведеном уредбом.

Запослени у Одсеку за информациони систем воде евиденцију о свим инцидентима, као и пријавама инцидената, у складу са наведеном уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 34.

У случају вандредних околности, које могу да доведу до измештања ИКТ система из просторија Завода, запослени са администраторским овлашћењима у Одсеку за информациони систем су дужни да у најкраћем року пренесу делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговањем у ванредним и кризним ситуацијама.

Спецификацију делова ИКТ система који су неопходни за фунционисање у ванредним ситуацијама израђује Одсек за информациони систем, и то у три примерка, од којих се један налази код дирекотра Завода, други код шефа Одсека за управање кадровима, планска документа и подршку управљању и опште послове и трећи код шефа Одсека за информациони систем.

Делови ИКТ система који нису неопходни за фунционисање у ванредним ситуацијама, складиште се на резервну локацију коју одреди директор Завода.

Сладиштење делова ИКТ система који нису неопходни се врше тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води.

III ПРОВЕРА ИКТ СИСТЕМА

Члан 35.

Проверу ИКТ система врше запослени са администраторским овлашћењима у Одсеку за информациони систем.

Проверу ИКТ система може вршити и лице изабрано у складу са законом којим се уређује поступак јавних набавки.

Провера ће се вршити последњег месеца у години.

Провера се врши тако што се:

1. проверава усклађеност Правилника о безбедности информационо-комуникационих система у Заводу, са прописаним условима, односно проверава да ли су адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;
2. проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима;
3. врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

О извршеној провери сачињава се извештај, који се доставља шефу Одсека за информациони систем и директору.

IV САДРЖАЈ ИЗВЕШТАЈА О ПРОВЕРИ ИКТ СИСТЕМА

Члан 36.

Извештај о провери ИКТ система садржи:

1. назив оператора ИКТ система који се провера;
2. време провере;
3. податке о лицима која су вршила проверу;
4. извештај о спроведеним радњама провере;
5. закључке по питању Правилника о безбедности информационо – комуникационих система у Заводу за интелектуалну својину са прописаним условима;
6. закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
7. закључке по питању евентуалних безбедносних слабости на ниову техничких карактеристика компоненти ИКТ система;
8. оцена укупног ниова информационе безбедности;
9. предлог евентуалних корективних мера;
10. потпис одговорног лица које је спровело проверу ИКТ система.

V ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Завода

Члан 37.

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

Ступање на снагу Акта о безбедности

Члан 38.

Овај Акт о безбедности ступа на снагу наредног дана од дана објављивања на интернет презентацији Завода.

Директор

Владимир Марић