ПОКРАЈИНСКИ ЗАВОД ЗА ЗАШТИТУ ПРИРОДЕ
Србија ■ 21000 Нови Сад ■ Радничка 20А
Тел: 021/4896-301 ■ Факс: 021/66-16-252
e-mail: novi.sad@pzzp.rs ■ www.pzzp.rs

INSTITUTE FOR NATURE CONSERVATION OF VOJVODINA PROVINCE
Serbia ■ 21000 Novi Sad ■ Radnicka 20A
Phone: +381214896301 ■ Fax: +381216616952
e-mail: novi.sad@pzzp.rs ■ www.pzzp.rs

Број: 02 010 2963/3

Датум: 20.10.2022.год

На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16, 94/2017 и 77/2019) и члана 2. Уредбе о ближем садржају аката о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Службени гласникРС", број 94/2016), те члана 12. Статута Покрајинског завода за заштиту природе (у даљем тексту Завод), Управни одбор Завода на 7. седници одржаној дана 20.11.2022. године доноси :

Акт о безбедности информационо-комуникационог система
Покрајинског завода за заштиту природе

I. ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система Покрајинског завода за заштиту природе (у даљем тексту: Акт о безбедности), у складу са Законом о информационој безбедности (у даљем тексту: Закон) и интерним процедурама које се односе на ИКТ систем, ближе се уређују се 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 Завода (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

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

Обавеза примене одредби Акта о безбедности

Члан 3.

Корисници ИКТ система Завода јесу запослени, лица ангажована на одређени период (привремени и повремени послови, праксе, пројекти и слично) као и трећа лица ангажована уговором за обављање послова у вези ИКТ система Завода (у даљем тексту ИКТ корисници).

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

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

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

За праћење примене овог правилника овлашћује се, као администратор ИКТ система, Пројектант информационих система и програма.

За контролу и надзор над обављањем послова ИКТ корисника, а у циљу заштите и безбедности ИКТ система задужени су запослени за послове администрирања ИКТ система Завода, док су непосредно надређени руководиоци (надаље: руководиоци) одговорни за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност запослених

Члан 4.

Мере прописане овим правилником се односе на све ИКТ кориснике.

ИКТ корисници су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања пословних активности из своје надлежности тј. ангажованости, 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, повлачи дисциплинску и материјалну одговорност корисника ИКТ система.

Одговорност покрећу руководиоци по пријави овлашћеног лица за прикупљање, анализу и обраду података о безбедности ИКТ система Завода.

Предмет заштите

Члан 5.

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

Информациона добра Завода су сви ресурси који :

- садрже пословне информације Завода, укључујући базе података и др. електронске записе,
- путем којих се врши израда, обрада, чување, претраживање, пренос, брисање и уништвање података у ИКТ систему,
- рачунарска опрема, преносни уређаји, и друга периферна опрема(штампачи, скенери, плотери, УПС уређаји и др.),
- оперативни системи, наменски креирани системи апликација, пословне апликације и сл,
- електронске комуникационе мреже.

Мере заштите

Члан 6.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, као и заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције на начин да интегритет, тајност и расположивост података не буду компромитовани.

Завод је у обавези набави и одржава потребу хардверску и софтверску опрему помоћу које ће се омогућити примена мера заштите предвиђених овим Актом.

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Завода

Члан 7.

Организациона структура представља скуп задатака и овлашћења којим се уређује начин на који ИКТ корисници обављају своје активности и користе расположиве ресурсе за постизање циљева организације. Завод у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

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

Пројектант информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода је задужено и одговорно за управљање информационом безбедношћу ИКТ система.

Директор или овлашћено лице Завода је дужан да донесе појединачни акт, у складу са актом о систематизацији, којим одређује одговорна лица за обезбеђивање и праћење безбедности ИКТ система. Сви ИКТ корисници морају бити упознати са процедуром заштите безбедности ИКТ система.

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

- Акт о безбедности ИКТ система Покрајинског завода за заштиту природе;
- Правилник о организацији и систематизацији радних места;
- Уговори о раду;
- Изјаве о поверљивости;

- Уговори о чувању поверљивости са правним лицима;
- Процедура за ажурирање корисничких налога;
- Процедура за сарадњу са сервисима опреме;
- Процедура о животном циклусу опреме;
- Правилник о коришћењу службених мобилних телефона и/или сим картица

Завод Процедуром за Ажурирање корисничких идентификација (налога) утврђује начин доделе овлашћења за приступ ИКТ систему, начин одобравања приступа запосленима од стране руководиоца, односно непосредно надређеног лица.

Члан 8.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара,
- праћење примена које могу утицати на опште стање заштите информација у Заводу,
- послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности,
- праћење активности и анализирање сигурносних инцидената у оквиру управљања информационом безбедношћу
- додељује улоге у поступку заштите,
- координирање и контрола примене мера заштите
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента Пројектант информационих система и програма, односно запослено лице на пословима администрирања ИКТ система Завода, обавештава директора, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Завод дозвољава рад на даљину и употребу мобилних уређаја од стране ИКТ корисника, 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.
Термин мобилни уређај укључује: преносиве рачунаре, мобилне телефоне, есктерне меморијске медијуме (диск, УСБ кључ, и слично).

Рад на даљину

Обављање послова ван просторија Завода је омогућавање обављања задатих и неопходних послова ван локалне рачунарске мреже Завода и обухвата:

- Рад на даљину - удаљени приступ ИКТ систему Завода;
- Рад од куће.

Удаљени приступ на ИКТ систем Завода (у седишту) омогућава се помоћу заштићене VPN конекције. Право на удаљени приступ, креирање налога за исти и инсталацију клијенског програм на мобилном уређају за реализацију истог, имају ИКТ корисници којима је он одобрен у складу са интерном Процедуром за Ажурирање корисничких идентификација (налога).

ИКТ корисници могу, путем мобилних уређаја, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности и ангажованости.

Правилном применом утврђеног поступка и начина приступа, Завод своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи.

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

За коришћење информатичких сервиса који су стандардно доступни преко интернета, као и електронске поште, нису потребне посебне сагласности.

Корисници ресурса ИКТ система којима је активан налог за службену електронску пошту, могу да приступе свом поштанском сандучету на маил серверу путем мобилних уређаја у власништву Завода или приватних уређаја, преко интернета (webmail). Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Пројектант информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода, контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава надређеног руководиоца Завода, а та MAC адреса се уноси у «block“ листу софтвера који се користи за контролу приступа.

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 за послове администрирања ИКТ система Завода. 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).

Коришћење мобилних уређаја од стране ИКТ корисника

Мобилни уређаји који користе запослени, морају бити претходно одобрени и/или набављени од стране Завода, и оцењени као компатибилни са захтевима обезбеђивања адекватног степена заштите од стране запосленог на пословима администрирања ИКТ система. ИКТ корисник којем је одобрено коришћење мобилног уређаја мора бити задужен за исти реверсом који је потписао (даље: задужени корисник).

Службени мобилни уређаји су у надлежности Завода и издају се запосленима ради коришћења приликом обављања службених обавеза. Задужени корисници имају право и обавезу да их користе у службене сврхе, да их користе са пажњом и чувају од оштећења или квара и евентуалних злоупотреба. Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Приликом коришћења мобилних уређаја мора се обезбедити заштита пословних података и смањити ризике коришћења мобилних уређаја у незаштићеним окружењима (јавним местима, мрежама са непознатом или недовољном заштитом и слично).

Задуженом кориснику је забрањена самостална инсталација софтвера и подешавање мобилног уређаја у власништву Завода, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.). За инсталације, подешавања и дијагностификовање нефункционалности задужено је лице запослено на пословима администрирања ИКТ система.

У случају квара уређаја, Задужени корисник је дужан да поступи у складу са интерном процедуром „Пријава нефункционалности рачунарске опреме и софтвера". Лице запослено на пословима администрирања ИКТ система је дужан/а да, уколико квар није такве врсте да то онемогућава, уради backup података који се налазе у уређају, затим квар или отклони или поступи у складу са интерном процедуром „Сарадња са сервисима рачунарске (и електронске) опреме", а по повратку из сервиса поново врати податке у мобилни уређај.

Задужени корисник мобилног уређаја путем којег је омогућен приступ мрежи Завода у обавези је да крађу или губитак мобилног уређаја пријави Пројектанту информационих система и програма односно запосленом лицу на пословима администрирања ИКТ система Завода без одлагања, а у року од 72 сата да достави писану изјаву о околностима крађе или губитка мобилног уређаја. Пројектант информационих система и програма односно запосленом лицу на пословима администрирања ИКТ система Завода је у обавези да, по пријави крађе или губитка мобилног уређаја, неодложно блокира несталом уређају приступ ИКТ систему Завода и кориснику промени креденцијале за приступ. У случају проналаска наведеног мобилног уређаја, Пројектант информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода ће извршити преглед уређаја и утврдити да ли он може поново бити коришћен.

3. 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 Завода управљају запослени у складу са важећом систематизацијом радних места.

Завод се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају.

Сви запослени и друга ангажована лица којима је на основу посебног уговора додељен приступ поверљивим информацијама, морају потписати изјаву о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура везаних за ИКТ систем 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.

Овај правилник ће бити истакнут на огласној табли и интернет страници Завода и сваки запослени или ангажовани корисник ИКТ ресурса је дужан да се упозна са одговорностима и правилима коришћења ИКТ ресурса Завода и да се упозна са правилима коришћења ресурса ИКТ система. У складу са тим и интерном процедуром „Ажурирање корисничких идентификација (налога)" свако запослено и ангажовано лице је дужно да потписаном изјавом

потврђује да је упознато са горе наведеним. Изјава се заводи и одлаже у лични досије потписаног лица.

ИКТ корисници у Заводу 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.

Сви запослени, извођачи радова и пословни партнери морају бити на одговарајући начин упознати са правилима и одговорностима за коришћење информација и опреме за процесирање информација и у обавези су да их се придржавају.

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

Члан 10.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања. Дужности и обавезе које остају важеће и после престанка запослења треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа.

Приликом престанка радног односа запосленог, преласка запосленог на друге послове или престанка сарадње са пословним партнером, потребно је да надлежни руководилац информише запосленог, односно пословног партнера, о свим захтевима везаним за заштиту информација и подсети га на законске обавезе из области заштите информација. Измена одговорности или промена послова морају се третирати као престанак тренутних одговорности, а нове одговорности разматрати као да се ради о запошљавању и закључењу новог уговора или споразума.

Приликом престанка запослења или ангажовања у Заводу а након поднетог захтева а у складу интерном процедуром „Ажурирање корисничких идентификација (налога)“, за поступања задужен је Пројектант информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода, који на основу дефинисаног захтева предузима следеће активности:

- прегледа све налоге и приступе систему који су били доступни запосленом и прикупља приступне шифре и кодове са циљем укидања/промене истих;
- на основу информација из захтева врши измене/укида приступне привилегије и налога електронске поште и свих других права приступа ИКТ систему ИКТ кориснику на ког се захтев односи;
- проверава враћене мобилне уређаје и уређаје за преношење података;
- преузима картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Завода.

О статусним променама ИКТ корисника и потреби предузимања наведених активности, лице запослено на радном месту- дипломирани правник за правне, кадровске и административне послове-шеф одсека, у сарадњи са непосредним руководиоцем, је дужно да обавести Пројектанта информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода, захтевом и у складу интерном процедуром „Ажурирање корисничких идентификација (налога)“, а у року од 2 дана од статусне промене.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида у складу интерном процедуром „Ажурирање корисничких идентификација (налога)“.

Завод мора да:

- на ИКТ добра примењује мере заштите прописне Законом о информационој безбедности и актима Завода,
- да мере заштите ИКТ добара примењује у складу са степеном осетљивости и критичности тих добара, узимајући у обзир могуће последице нарушавања поверљивости, интегритета и расположивости добара.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра Завода 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 на ИКТ систем и сл.
Завод врши идентификацију имовине која одговара животном циклусу добара/информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација, а у складу са Листом категорија регистратурског материјала са роковима чувања. Завод прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином, а у складу са Правилником о попису имовине. Евиденцију о информационим добрима води Пројектант информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода, у папирној или електронској форми.
Предмет заштите су:

- хардверске и софтверске компоненте ИКТ система
- подаци који се обрађују или чувају на компонентама ИКТ система
- кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система Завода

6. Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности

Члан 12.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебним прописима.

Избор и ниво примене мера заштите података се заснива на процени ризика, потреби за превенцијом ризика и отклањању последица ризика који се остварио, укључујући све врсте ванредних околности.

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Службени гласник РС“, број 53/2011).

7. Заштита носача података

Члан 13.

Пројектант информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информације и садржаја који се чувају на носачима података и имају посебан значај за функционисање ИКТ система.

Пројектант информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода, ће успоставити организацију приступа и рада са подацима посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података , тако да:

- 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-корисници којима је то право обезбеђено одлуком директора,
- подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника.

Обавезно је минимизовати коришћења преносних медијума. Пре коришћења преносни носачи информација морају се подвргнути провери средствима за заштиту од злонамерног софтвера.

Приликом рада са носиоцима података корисници се придржавају следеће процедуре:

Корисник је дужан да процени поузданост носиоца података – поуздани носиоц је онај који је обезбедио Завод.

Корисник у току рада мора да има надзор над носиоцем података у сваком тренутку. Не сме се остављати носиоц података доступан другим лицима, како би се спречила могућност да дође до читања или уписа података од стране неовлашћеног лица. –

По завршетку рада корисник одјављује носиоц података са система и лично води рачуна о безбедности носиоца података или га предаје на чување Пројектанту информационих система и програма односно запосленом лицу на пословима администрирања ИКТ система Завода.

У случају нестанка носиоца података у најкраћем року обавештава Пројектанта информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода.

Евиденцију носача на којима су снимљени подаци, води Пројектант информационих система и програма односно запослено лице на пословима администрирања ИКТ система Завода 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, директора Завода 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.

8. Ограничење приступа подацима и средствима за обраду података

Члан 14.

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

Корисницима се додељују минимална права приступа и привилегије за приступ ИКТ добрима, потребна за обављање пословних задатака, укључујући у то и приступ рачунарској мрежи и мрежним ресурсима.

- Ограничење приступа подразумева:
- физичку контролу приступа (браве)
- административно ограничење приступа (раздвајање надлежности)
- техничка контрола приступа (корисници система са дефинисаним врстама приступа у оквиру мрежних уређаја, логови догађаја у систему, софтвер за заштиту од злонамерног софтвера, бекап података и слично).

Ограничење приступа врши се у складу са улогом корисника ИКТ система. Све методе контроле приступа морају се разматрати заједно. Приступ се ограничава уређајима које корисник користи за приступ информационим и техничким ресурсима. Контрола минимално подразумева аутентикацију корисника и контролу приступа информационим услугама.

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

ИКТ корисник може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, сем администратору за подешавање корисничког профила, радне станице или других дељених реурса ИКТ система.

ИКТ корисник, у свакодневном раду користи радну станицу коју је администратор подесио за послове конкретног корисника. Изузетно, може да приступи радним станицама других ИКТ корисника уз одобрење директора или одобрење помоћника директора, о чему треба да буде обавештен и да има сазнање ИКТ корисник који у свакодневом раду користи предметну радну станицу и према чијим пословима је подешена.

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

ИКТ 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 креденцијале/налоге (корисничко име и лозинку), 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;

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 службену електронску пошту у складу са прописаним процедурама;

14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање оперативних система и 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.

17) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 15.

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

Право приступа имају само ИКТ 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 само Пројектант информационих система и програма односно лице на пословима администрирања ИКТ система Завода. Привилегована права на приступ која треба доделити корисничком налогу другачија су од оних која се користе за редовне активности. Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора.

Забрањено је неовлашћено коришћење администраторских корисничких налога.

Лозинке за администраторске корисничке налоге морају бити промењене са променом администратора.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу кога/јих се врши

аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране ИКТ корисника.

Корисничко име и лозинке се морају користити као стандардно средство за верификацију идентитета корисника пре давања приступа информационом систему или услузи, у складу са овлашћењима корисника. Приступ оперативном систему омогућен је корисницима тек након што прођу процедуруе идентификације и аутентификације

Кориснички налог додељује администратор, на основу захтева у складу интерном процедуром „Ажурирање корисничких идентификација (налога)“ и потребама обављања пословних задатака од стране ИКТ корисника.

Кориснички налог може да се креира и на основу квалификованог електронског сертификата, уколико су испуњени технички услови за такав систем аутентификације.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева у складу интерном процедуром „Ажурирање корисничких идентификација (налога)“.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 16.

Аутентификације корисника којима је одобрен приступ ИКТ систему врши се путем јединственог корисничког налога, акоји се састоји од корисничког имена и лозинке.

Лозинка мора да садржи минимум шест карактера комбинованих од малих и великих слова, цифара и специјалних знакова.

Лозинке не заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и друге препознатљиве податке.

Корисници су дужни да привремене шифре промене приликом првог пријављивања и најмање једном у шест месеци. Иста лозинка се не сме понављати у временском периоду од годину дана.

Сви корисници су дужни да додељено корисничко име и шифру држе у тајности, избегавају чување корисничког имена и шифре у писаном облику и не откривају их другим лицима, укључујући и надређене особе Ако ИКТ корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 17.

Завод у свом пословању нема података које треба да заштити криптографски.

Област у којој се користи криптографска заштита је дигитални потпис ради потврде аутентичности документа и ауторизација приступа сервисима других институција.

Дигитални потпис и ауторизација приступа сервисим се користи у складу са правилима издаваоца дигиталног сертификата

Запослена лица на пословима администрирања ИКТ система Завода су задужена за инсталацију потребних уређаја и апликација за коришћење сертификата.

ИКТ корисници су дужни да чувају своје квалификоване електронске сертификате и не учине их доступним другим лицима.

12. 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, централна мрежна или комуникациона опрема ИКТ система (даље: сервер сала), и/или у којима се налазе документи 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.

Завод је дужан да предузме радње за спречавање неовлашћеног физичког приступа административној зони.

Простор мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (константно климатизован простор). Непосредно уз простор или у њему, мора се налазити противпожарна опрема, која се може користити само у случају пожара у сервер сали.

Административној зони овлашћени су приступити Пројектант информационих система и програма односно лице на пословима администрирања ИКТ система Завода (овлашћена лица), који:

- Дуже један примерак кључа од сервер сале,
- Воде евиденцију о уласку у сервер салу, а на основу евиденције физичко техничког особља који су одговорни за други примерак кључа од сервер сале и обавезно евидентирају предају кључа,
- Проверавају услове околине у сервер сали.

У случају да је потребан приступ административној зони лицу које није овлашћено лице (нпр. Хигијенско одржавање, одржавање опреме, сервисирање, непредвиђене околности…) то може учинити уз присуство/сагласност овлашћеног лица.

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

Члан 19.

Неопходно је заштитити средства која чине ИКТ систем од губитка, оштећења, крађе или другог облика угрожавања безбедности. У циљу заштите средстава, неопходно је водити рачуна о постављању средстава на безбедна места, елиминисати непотребан приступ у простор у коме се налазе, вршити редовне провере заштићености средстава од крађа, пожара, и других претњи и пратити услове околине (температура, влажност и др.) који би могли негативно да утичу на рад средстава.

Прилаз административној зони, дозвољен је само Пројектанту информационих система и програма односно лицу на пословима администрирања ИКТ система Завода.

Осим наведених, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система и одржавања просторије или пратећих уређаја у

њој, а по претходном одобрењу директора или помоћника директора Завода и уз присуство Пројектанта информационих система и програма односно лица на пословима администрирања ИКТ система Завода.

Сервери и активна мрежна опрема (switch, modem, router, firewall), морају стално бити прикључени на уређаје за непрекидно напајање – UPS. У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, овлашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења.

У случају изношења опреме ради селидбе, неопходно је одобрење директора или помоћника директора Завода који ће одредити услове, начин и место изношења опреме.

Техничка средства се морају одржавати у складу са експлоатационом документацијом и упутством произвођача како би се осигурала непрекидна расположивост и интегритет података

Ако се опрема износи ради сервисирања, поред одобрења директора или помоћника директора Завода, потребно је сачинити записник/реверс у коме се наводи инвентарни број, назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера. У случају сервисирања опреме мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Завода.

Складишни простор за резервне копије података мора бити у простору удаљеном од сервер сале.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 20.

Пројектант информационих система и програма односно лице на пословима администрирања ИКТ система Завода, 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 директору и помоћнику директора Завода одговарајуће мере.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву 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.

При тестирању софтвера, опреме или комуникационих саобраћајница, потребно је обезбедити неометано функционисање ИКТ система. Забрањено је коришћење продукцијских сервера за тестирање нових софтверских/комуникационих решења, на начин који може да угрози нормално функционисање ИКТ система Завода.

15. Заштита података и средства 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 (USB меморија, CD итд.), инсталацијом нелиценцираног

софтвера и сл. За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм, који мора имати могућност континуираног аутоматског ажурирања антивирусних дефиниција. Забрањено је заустављање, искључивање и неовлашћено подешавање антивирусног софтвера.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса. Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија. 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.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени-корисник прикључује на Интернет мора бити одговарајуће подешен од стране Пројектанта информационих система и програма односно лица запосленог на пословима администрирања ИКТ система Завода. Заштиту од вируса и упада са интернета у ИКТ систем Завода је обезбеђена заштитним зидом, који надгледа администратор. Приликом коришћења интернета заштитни зид блокира познате опасне и сумњиве WEB странице, с обзиром да то може проузроковати проблеме - неприметно инсталирање шпијунских програма и слично.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави администратору ИКТ система Завода.

Анализирати случајеве продирања и имплементације злонамерног софтвера у оквиру мера за управљање инцидентима информационе безбедности.

Без обзира што је једна од функционалности заштитног зида, ИКТ корисници треба да буду свесни да је строго забрањено гледање филмова и играње игрица на рачунарима и претраживање WEB страница које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

Недозвољена употреба интернета обухвата:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин; • нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимање (download) података велике “тежине” које проузрокује “загушење” на мрежи;
- преузимање (download) материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

Овлашћење за приступ друштвеним мрежама у пословне сврхе омогућује Пројектант информационих система и програма односно лице запослено на пословима администрирања ИКТ система Завода, након одобрења директора или помоћника директора.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (нпр. Прикључивање преко сопственог модема), осим у случају прикључивања путем VPN конекције.

Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже може се одузети право приступа.

16. Заштита од губитка података

Члан 22.

Завод 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.

Израђују се :

- Резервне копије база података (основна делатност, општи послови, финансијски и просторни подаци),
- Резервне копије целокупног серверског система (за сваки сервер).

Архивирање база података се врши најмање једном дневно, са посебно издвојеном и обезбеђеном месечном и годишњом копијом, за потребе обнове базе или мигрирања података на нову платформу.

Подаци о запосленима-корисницима се архивирају кроз копију базе која је саставни део информационог система Завода.

Дневне копије база чувају се најмање седам дана.

Месечна копија база података обухвата стање података на дан последњег дана у месецу, архивира се на оптичком медију и одлаже у сеф који обезбеђује адекватно чување медија. Месечне копије база података чувају се најмање годину дана.

Годишња копија база података обухвата стање података на дан последњег дана у години, архивира се на оптичком медију и одлаже у сеф који обезбеђује адекватно чување медија. Годишње копије база података чувају се у року одређеном у Упутству о канцеларијском пословању органа државне управе („Сл. Гласник ПС“, бр 10/93, 14/93-испр. И 67/2016, 3/2017 и 20/2022- др.упутство).

Сваки примерак оптичког медија са месечним/годишњим копијама-архивама, мора бити означен информацијама: врста (месечна, годишња), датум стања података копије-архиве, садржај архиве (копије за коју базу су на медију) и именом запосленог који је израдио архиву. Носиоци копије-архиве база података одлажу у сеф који обезбеђује адекватно чување медија.

Резервне копије целокупног серверског система треба да обезбеде повратак серверског система у случају инцидента који је нарушио функционалност сервера или интегритет података.

Резервне копије целокупног серверског система се израђују свакодневно, системом намењеном за израду копија и повратак система из истих, и то у два примерка:

- Прва копија се смешта на спољни диск за ту намену
- Друга копија (копија копије) се смешта на складишни уређај (НАС) који је на локацији удаљеној од сервер сале.

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

Неопходно је периодично проверавати исправност копија података и система.

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

Члан 23.

У ИКТ систему Завода формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу, у складу са обезбеђеним софтвером за ту намену.

Завод прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са - информационом безбедношћу, који се морају чувати и редовно преиспитивати. Администратори система немају дозволу да бришу или деактивирају дневнике о сопственим активностима..

Пројектант информационих система и програма односно лице запослено на пословима администрирања ИКТ система Завода стара се о чувању генерисаних записа о догађајима, активностима корисника (корисничког налога), и грешкама у вези са безбедношћу информација.

Систем за контролу и дојаву о грешкама и неовлашћеним активностима мора бити подешен тако да одмах обавештава администраторе ИКТ система о свим нерегуларним активностима корисника и о покушајима упада и упадима у систем.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Завода или софтвер отвореног кода и са лиценцом која не ограничава/забрањује коришћење наведеног од стране Завода.

Инсталацију и подешавање софтвера може да врши само Пројектант информационих система и програма односно лице запослено на пословима администрирања ИКТ система Завода.

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

Пре сваке инсталације нове верзије софтвера, односно подешавања, неопходно је водити рачуна о могућности повратка на претходно стање у случају неочекиваних ситуација.

У циљу одржавања исправности софтвера врше се мере отклањања слабих тачака софтвера. Отклањање слабих тачака софтвера се постиже редовним инсталирањем нових верзија софтвера. Ажурирање оперативних ситема и другог опште-системског и апликативног софтвера врши Пројектант информационих система и програма односно лице запослено на пословима администрирања ИКТ система Завода.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

У циљу правовременог и ефикасног реаговања на објављене и уочене слабе тачке софтвера се предузимају мере за контролу заштићености средстава за обраду, чување и предају информација.

Контролу заштићености врши Пројектант информационих система и програма односно лице запослено на пословима администрирања ИКТ система Завода на следећи начин:

- периодичном анализом заштићености помоћу скенерања безбедносним алатима/софтверима,
- мониторингом заштићености,
- анализом конфигурационих фајлова средстава за обраду, чување и пренос информација.

Подаци о слабим тачкама софтверских решења редовно се обнављају са сајтова произвођача конкретних решења. Уочене слабе тачке средстава за обраду, чување и пренос информација отклањају се помоћу нових верзија софтвера („update“) или применом препоручених конфигурација које нуде произвођачи софтвера.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, Пројектант информационих система и програма односно лице запослено на пословима администрирања ИКТ система Завода је дужан/а да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости, или предложи ангажовање трећег лица директору или помоћнику директора Завода.

Потребно је да се путем подешавања корисничких полиса, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

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

Члан 26.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе Завода, је да предузете активности имају што мањи утицај на функционисање система, тако што планира адекватно време спровођења ревизије и редослед активности који не ометају пословне процесе унутар ИКТ система..

Ревизија ИКТ система се врши уз претходну сагласност директора или помоћнику директора Завода.

Ревизија ИКТ система врши се по правилу ван радног времена, осим када је у питању хитност потребе за њом.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 27.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или у каналицама, тако да онемогуће неовлашћени приступ и оштећење.

Активна мрежна опрема се мора налазити у закључаним ормарима наменски креираним за ову намену.

Пројектант информационих система и програма, односно лице запослено на пословима администрирања ИКТ система Завода је дужан/а да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности

За спровођење провера постојања адекватне безбедности мрежних сервиса ангажују се фирме које се баве одржавањем мрежа рачунара. Комуникационим мрежама треба адекватно управљати и контролисати их, како би се оне заштитиле од претњи, да би се одржала сигурност система и апликација које користе мрежу, укључујући и заштиту информације које су у протоку. Приликом закључивања уговора о мрежним услугама, за све мрежне услуге треба идентификовати ризике и узети у обзир елементе заштите информација да се ризици минимизују.

Бежична мрежа коју могу да користе лица која нису ИКТ корисници Завода, мора бити одвојена од интерне мреже кроз коју се одвија саобраћај у службене сврхе.

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

Члан 28.

Електронска пошта се може користити искључиво за пословне потребе. Није дозвољено корисничке налоге додељене пословну упоребу користит за регистровање на друштвеним мрежама и другим порталима, изузев у пословне сврхе.

Електронском поштом не смеју се дистрибуирати подаци чија компромитација може да угрози безбедност ИКТ система Завода.

Заштита података који се преносе комуникационим средствима између Завода и трећег лица обезбеђује се поштовањем Споразума о преносу информација којим су утврђена правила и процедуре размене података и применом адекватних контрола.

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

Члан 29.

Информациона и техничка решења обухватају оперативне системе, инфраструктуру, пословне апликације, ИТ услуге других лица, готове софтверске пакете и хардвер.

Приликом увођење новог подсистема за обраду информација морају бити укључени захтеви који се односе на безбедност информација као и да имплементација новог система не нарушава постојећи систем заштите информација, функционисање и неопходне перформансе ИКТ система.

Примена мера заштита информација је обавезна током целог животног века информационих и техничких решења у:

- фази пројектовања,
- фази обезбеђења буџета,
- фази поступка набавке,
- фази поступка уговарања,
- фази експолатације,
- фази поступка измене или унапређења постојећег система и
- фази поступка престанка са коришћењем система.

Пројектант информационих система и програма проверава примену мера заштите у свим наведеним фазама.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Заводу, дефинише се уговором склопљеним са тим лицем,

обавезно са ставкама која се односе на: безбедност постојећег ИКТ систем Завода, тестирање и имплементацију наведеног.

Пројектант информационих система и програма је задужен/а за технички надзор над реализацијом уговорених обавеза од стране трећих лица, што се записнички констатује.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система запослени из претходног става води документацију.

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

Члан 30.

За потребе тестирања ИКТ система односно делова система користе се подаци који нису осетљиви, који се штите, чувају и контролишу на одговарајући начин.

Апликације и софтвер оперативног система је потребно имплементирати тек после успешно спроведеног тестирања, којим треба обухватити проверу применљивости, сигурности, утицаја на друге системе и погодности за коришћење.

Током тестирања избегавати коришћење продукционих база података које садрже осетљиве информације. Ако се за сврху испитивања користе информације о личности или неке друге осетљиве информације, неопходно је применити мере заштите информација као на стварним, продукционим системима у складу са прописима и овлашћењима.

Приступ изворном програмском коду и припадајућим информацијама строго контролисати, како би се спречило увођење недокументованих и неауторизованих функција, као и да би се избегле ненамерне промене.

Пројектант информационих система и програма је задужен/а за технички надзор над тестирањем.

25. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 31.

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима који се налазе у базама података којима приступа софтвер/платформа који су они израдили, односно за које постоји уговором дефинисан приступ.

Размену информација и софтвера са пословним партнерима заснивати на званичној политици размене, регулисане одговарајућим уговорима, односно споразумима.

Коришћење екстерних организација за управљање информационим и техничким ресурсима представља сигурносни ризик, те је неопходно унапред извршити процену ризика, припремити одговарајуће мере заштите.

Ангажовани од стране Пословног партнера не могу имати права администрирања која су потребна за промену параметара аутентификације, ауторизације и права приступа. Током пружања услуга, ангажовани од стране Пословног партнера, морају имати минимална права потребна за обављање послова, а која нису у супротности са претходним ограничењима.

Морају се применити следеће мере:

употреба персонализованих корисничких налога (име и презиме);

удаљени приступ остваривани искључиво путе VPN конекције формиране од стране запосленог Пројектанта информационих система и програма односно лица запосленог на пословима администрирања ИКТ система Завода на којој се бележе све активности у дневницима (логовима).

Мере заштите које се примењују приликом приступа лица запослених преко фирми које пружају услуге изнајмљивања људских ресурса идентичне су мерама заштите које се примењују на ИКТ кориснике у Заводу. У свим фазама рада са информационим и техничким ресурсима, треба обезбедити могућност контроле и увида у активности ангажованих екстерних организација.

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

Члан 32.

У циљу одржавања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, неопходно је успоставити механизме надзора над пружањем услуга. Пројектант информационих система и програма задужен/а је за надзор над поштовањем уговорених обавеза и праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности.

У случају непоштовања уговорених обавеза Пројектант информационих система и програма је дужан/дужна да одмах обавести директора или помоћника директора, како би предузели мере у циљу отклањања неправилности.

27. 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-корисник је дужан да одмах обавести Пројектанта информационих система и програма (односно лице запослено на пословима администрирања ИКТ система Завода.

По пријему пријаве Пројектанта информационих система и програма односно лица запосленог на пословима администрирања ИКТ система Завода је дужан/а да одмах обавести помоћника директора Завода и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Сл. Гласник РС“, бр, 94/2016), запосленог Пројектанта информационих система и програма односно лица запосленог на пословима администрирања ИКТ система Завода је дужан/а да обавести и надлежни орган дефинисан овом уредбом.

Пројектант информационих система и програма води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са Уредбом, на основу које могу да се воде дисциплински, прекршајни и кривични поступци против одговорног лица.

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 34.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Завода, Пројектант информационих система и програма се стара да у најкраћем року пренесе

делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује Пројектант информационих система и програма (шифра ГО40300), и то у три примерка, од којих се један задржава за себе, други дистрибуира запосленом надлежном за послове одбране и ванредне ситуације а трећи римерак директору Завода.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди директор или помоћник директора Завода. Складиштење делова ИКТ система који нису неопходни, се врши 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 врши Пројектант информационих система и програма или треће лице ангажовано уговором.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на које се врши упућивање, са прописаним условима, односно проверава да ли су правилником 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, методама интервјуа, симулације, посматрања, увида у предвиђене евиденције и другу документацију;

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 помоћнику директора и директору Завода.

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава;

2) време провере;

3) подаци о лицима која су вршила проверу;

4) извештај о спроведеним радњама провере;

5) закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;

6) закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;

7) закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система;

8) оцена укупног нивоа информационе безбедности;

9) предлог евентуалних корективних мера;

10) потпис одговорног лица које је спровело проверу ИКТ система.

IV. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Завода

Члан 36.

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

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, Пројектант информационих система и програма (шифра ГО40300) је дужан/а да обавести помоћника директора и директора Завода, како би могли да приступе измени овог правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Ступање на снагу Акта о безбедности

Члан 37.

Ступањем на снагу престаје да важи Правилник о безбедности информационо-комуникационог система бр 04 503 од 28.02.2019. године.

Члан 38.

Овај Правилник ступа на снагу осмог дана од дана дана доношења, објављивањем на огласној табли Завода.

Председник управног одбора