На основу члана 7 и 44 Закона о државној управи („Службени гласник РС“, бр. 79/05, 101/07, 95/10, 99/14), члана 8, став 1 Закона о информационој безбедности („Службени гласник РС“, број 6/16), члана 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), члана 26 Закона о министарствима („Службени гласник РС“, бр. 44/14, 14/15, 54/15, 96/15 – др. закон, 62/17), чланова 7 и 8 Закона о званичној статистици („Службени гласник РС“, број 104/09, 24/11), директор Републичког завода за статистику доноси

ПРАВИЛНИК
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА РЕПУБЛИЧКОГ ЗАВОДА ЗА СТАТИСТИКУ

I. УВОДНЕ ОДРЕДБЕ

Члан 1

Правилником о безбедности информационо-комуникационог система Републичког завода за статистику (у даљем тексту: Правилник о безбедности), у складу са Законом о информационој безбедности („Службени гласник РС“, број 6/16) 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), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система (у даљем тексту: ИКТ систем) Републичког завода за статистику (у даљем тексту: Завод).

Циљеви Правилника о безбедности

Члан 2

Циљеви доношења Правилника о безбедности су:

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

Обавеза примене одредаба Правилника о безбедности и одговорност лица која приступају ИКТ систему

Члан 3

Примена одредаба овог правилника је обавезна за све запослене у Заводу, друга лица која су радно ангажована од стране Завода, као и све кориснике информатичких ресурса Завода (у даљем тексту: корисници ИКТ система), а који морају бити упознати са садржином Правилника о безбедности и поступати у складу с његовим одредбама, као и одредбама других интерних процедура које регулишу информациону безбедност.

Непоштовање одредаба Правилника о безбедности повлачи дисциплинску, прекршајну или кривичну одговорност корисника ИКТ система Завода.

Поједини термини ИКТ система

Члан 4

Поједини термини, који се користе у функционисању ИКТ система, имају следеће значење:

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

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

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

(в) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачке (а) и (б) ове тачке, у сврху њиховог рада, употребе, заштите или одржавања;

(г) организациону структуру путем које се управља ИКТ системом;

2) **информациона безбедност** представља 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, под контролом овлашћених лица;

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

4) **интегритет** значи очуваност изворног садржаја и комплетности података;

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

6) **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;

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

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

9) **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;

10) **инцидент** је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

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

12) **тајни податак** од интереса за Републику Србију је податак који је законом, другим прописом или одлуком надлежног органа, донесеним у складу са законом, одређен и означен одређеним степеном тајности;

13) **ИКТ систем за рад са тајним подацима** је ИКТ систем који је, у складу са законом, одређен за рад са тајним подацима;

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

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

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

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

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

19) **безбедносна зона** је простор у коме се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

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

21) **бекап** је резервна копија података;

22) **архивирање података** је процес складиштења посебно одабраних података за дугорочно чување и њихово будуће референцирање;

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

24) **MAC адреса** *(Media Access Control Address)* јесте јединствени број, којим се врши идентификација уређаја на мрежи;

25) **download** је трансфер података са централног рачунара или веб-презентације на локални рачунар;

26) **UPS** *(Uninterruptible power supply)* је уређај за непрекидно напајање електричном енергијом;

27) **freeware** је бесплатан софтвер;

28) **open-source** је софтвер отвореног кода;

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

30) **USB, CD-ROM, DVD, флеш меморија, екстерни хард-дискови, касете** јесу спољашњи медијуми за складиштење података.

II. МЕРЕ ЗАШТИТЕ

Члан 5

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности Завода а посебно у оквиру пружања услуга другим лицима.

Описи мера заштите груписани су у 28 одељака, према називима и редоследу тачака из члана 7, став 3 Закона о информационој безбедности.

1. Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Завода

Члан 6

Сваки корисник ресурса ИКТ система Завода је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности. Завод у оквиру организационе структуре утврђује послове и одговорности корисника ИКТ система ради управљања информационом безбедношћу.

Најзначајнији интерни документи који се баве уређењем обавеза и одговорности корисника ИКТ система у вези са управљањем информационом безбедношћу су:

- Правилник о унутрашњем уређењу и систематизацији радних места у Заводу;
- Правилник о начину коришћења и давања података које производи Завод;
- Правилник о заштити статистичких података у Заводу;
- Правилник о архивирању и бекапу електронских података у Заводу;
- Стратегија развоја информисања и дисеминације;
- ИКТ стратегија;
- Процедура за приступ подацима које је Завод преузео из других административних извора;

– Политика објављивања;
– Упутство о мерама заштите података и информација у Заводу;
– Упутство о начину коришћења „Заштићене просторије“;
– Наредба о поступању сагласно законским прописима у вези са неовлашћеним давањем статистичких података.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност;
- послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности;
- 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;
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу;
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

2. Постизање безбедности рада на даљину и употреба мобилних уређаја

Члан 7

Завод дозвољава рад на даљину и употребу мобилних уређаја од стране корисника ИКТ система, уколико је осигурана безбедност рада у случају обављања послова ван Завода, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења, крађе и губитка мобилних уређаја. Уређаји у Заводу морају бити подешени тако да омогуће сигуран и безбедан приступ ИКТ систему коришћењем VPN и уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера. Приступ ресурсима ИКТ система је под контролом надлежне организационе јединице.

Кориснички уређаји са којих ће се приступати ресурсима ИКТ система, могу се користити само за обављање послова у надлежности корисника ИКТ система и то само у периоду када није могуће користити уређај у власништву Завода.

Корисницима ИКТ система, забрањена је самостална инсталација софтвера и подешавање службеног мобилног уређаја, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.).

Рад на даљину

Омогућавање обављања задатих и неопходних послова на даљину уређује се путем процедуре за VPN приступ информационом систему Завода.

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

Сви пословни подаци који се креирају приликом рада на даљину, складиште се у информационом систему.

Коришћење мобилних уређаја

Мобилни уређаји подразумевају све преносне електронске уређаје намењене за комуникацију на даљину. У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони и сви други мобилни уређаји.

Право на коришћење мобилних уређаја ван Завода стиче се писменим одобрењем од стране надлежних лица Завода.

У случају крађе или губитка мобилног уређаја, сваки корисник ИКТ система је дужан да то одмах пријави надлежном лицу Завода.

3. Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност

Члан 8

ИКТ системом управљају запослени у складу са додељеним овлашћењима и одговорностима.

Сви корисници ИКТ система којима је додељен приступ поверљивим информацијама, морају потписати изјаву да су упознати са правилима коришћења ИКТ ресурса пре него што им се дозволи приступ опреми за обраду информација и морају бити упознати са овим правилником.

Свако коришћење ИКТ ресурса Завода од стране корисника ИКТ система мимо прописаних правила и процедура, као и додељених овлашћења, подлеже дисциплинској, прекршајној или кривичној одговорности, којом се дефинише одговорност за неовлашћено коришћење имовине.

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

Члан 9

Сви корисници ИКТ система су дужни да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система Завода и након престанка или промене радног ангажовања. Промена привилегија ће се извршити у складу са описом радних задатака а на основу захтева претпостављеног руководиоца.
У случају престанка радног ангажовања запосленог односно престанка коришћења ИКТ система од стране других корисника, поступа се по утврђеној процедури.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10

Информациона добра Завода су сви ресурси који садрже пословне информације, 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 компоненти, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем и сл.

Предмет заштите су:

- хардверске и софтверске компоненте ИКТ система;
- апликације и сервиси Завода;
- подаци који се обрађују или чувају на компонентама ИКТ система;
- кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система;
- комуникациони линкови.

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

Члан 11

Подаци који се налазе у ИКТ систему представљају пословну тајну ако су тако дефинисани одредбама посебних прописа (Закон о слободном приступу информацијама од јавног значаја („Службени гласник РС“, бр. 120/04, 54/07, 104/09 и 36/10), Закон о заштити података о личности („Службени гласник РС“, бр. 97/08,104/09 – др. закон 68/12, одлука УС и 107/12), Закон о тајности података („Службени гласник РС“, број 104/09), Уредба о начину и поступку означавања тајности података, односно докумената („Службени гласник РС“, број 8/11), и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Службени гласник РС“, број 53/11).

7. Заштита носача података

Члан 12

Завод обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података. Подаци и њихови носачи, посебно они који су означени степеном службености или тајности, штите се у складу са Законом о тајности података.
Заштита података и њихових носача обезбеђује се и процедурама које се поштују током рада а које доприносе следећем:

- да се подаци и документи (посебно они са ознаком тајности) снимају на сервере, у фолдере над којима ће право приступа имати само запослени односно корисници којима је то право одобрено;
- да се подаци и документи (посебно они са ознаком тајности) снимају и на друге носаче (екстерни хард-диск, USB, CD, DVD), над којима ће право приступа имати само корисници ИКТ система којима је то право одобрено.

8. Ограничење приступа подацима и средствима за обраду података

Члан 13

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеним овлашћењима коју корисници ИКТ система имају.

Запослени који имају администраторски налог, имају право приступа ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) ради инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Корисници ИКТ система могу да користе само свој кориснички налог који су добили од администратора система и не смеју да омогуће другом лицу коришћење његовог корисничког налога, сем администратору система, за подешавање корисничког профила и радне станице.

Уколико на било који начин злоупотребљавају права, односно ресурсе ИКТ система, подлежу дисциплинској, прекршајној или кривичној одговорности.

Корисници ИКТ система су дужни да поштују и следећа правила безбедног и примереног коришћења ресурса ИКТ система, и то:

1) да користе информатичке ресурсе искључиво у пословне сврхе;

2) да прихвате 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) да поступе са поверљивим подацима у складу са прописима а посебно приликом копирања и преноса података;

4) да безбедно чувају своје лозинке, односно да их не преносе другим лицима;

5) да мењају лозинке сагласно утврђеним правилима;

6) да поднесу захтев за инсталацију софтвера или хардвера у писаној форми, одобрен од стране непосредног руководиоца;

7) да обезбеде сигурност података у складу са важећим прописима;

8) да приступе информатичким ресурсима само на основу експлицитно додељених корисничких права;

9) да не заустављају рад и не бришу антивирусни програм, не мењају његове подешене опције, не инсталирају неовлашћено други антивирусни програм;

10) да не складиште садржај на радној станици, не складиште садржај који не служи у пословне сврхе;

11) да израђују заштитне копије (бекап) података у складу са прописаним процедурама;

12) да користе интернет и електронску пошту у складу са прописаним процедурама;

13) да прихвате да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;

14) да прихвате да сви приступи информатичким ресурсима и информацијама буду засновани на принципу минималне неопходности;

15) да прихвате да технике сигурности (антивирусни програми, заштитни зидови – *firewall*, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;

16) да не инсталирају, не модификују, не искључују из рада или бришу заштитни, системски или апликативни софтвер.

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

Члан 14

Право приступа ИКТ систему Завода имају сви корисници ИКТ система који приступају заштићеним ресурсима из пословних разлога.

Они имају имају само један доменски налог којим приступају свим ресурсима који су неопходни за обављање пословних задатака.

Налог се састоји од корисничког имена и лозинке, на основу којих се врши аутентификација (провера идентитета) и ауторизација (провера права приступа, односно права коришћења ресурса ИКТ система од стране корисника ИКТ система).

Налози могу бити администраторски и кориснички.

Администраторски налог је налог преко кога администратор система води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог на пословима управљања људским ресурсима, односно захтева надлежног руководиоца.

Кориснички налог је налог који додељује администратор система, на основу захтева запосленог задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем, и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима, а у складу са потребама обављања пословних задатака од стране корисника ИКТ система.

Сваком кориснику ИКТ система се додељује право на приступ ИКТ систему у складу са радним задацима које обавља. Такође му се додељују и јединствени подаци за логовање, који се не смеју делити са другим корисницима.
Привилегована права на приступ која треба доделити неком кориснику ИКТ система, другачија су од оних која се користе за редовне активности. Компетенције корисника са привилегованим правима на приступ редовно се преиспитују ради провере да ли су у складу са обавезама корисника.

Корисницима ИКТ система који имају приступ информацијама и опреми за обраду информација, по престанку запослења или истеку уговора, укида се право на приступ ИКТ систему.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15

Аутентификација корисника којима је одобрен приступ систему врши се путем корисничког имена и лозинке.

Сви корисници ИКТ система су дужни:

- да привремене шифре промене приликом првог пријављивања;
- да корисничко име и лозинку држе у тајности и не откривају их другим лицима, укључујући и надређене особе;
- да избегавају чување корисничког имена и лозинке у писаном облику;

- да промене лозинку увек када постоји било какав наговештај могућег компромитовања.

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

Члан 16

У Заводу није предвиђена криптозаштита података.
Ради заштите тајности, аутентичности и интегритета података, Завод може да размотри коришћење одговарајућих мера криптозаштите.

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

Члан 17

С циљем физичке сигурности информатичких ресурса морају се обезбедити следећи услови:

1) одговарајућа физичка заштита свих објеката у којима се налазе средства и документација ИКТ система;
2) сервери, мрежна и комуникациона опрема ИКТ система, као и средства и документација ИКТ система, место где се врши обрада података у ИКТ систему, морају бити смештени у посебном простору (сервер сали), који испуњава стандарде противпожарне заштите, који има климатизацију и који је адекватно чуван;
3) сервер сала мора бити примерено физички обезбеђена са двадесетчетворочасовним дежурством свих седам дана у недељи, с циљем детекције и онемогућавања физичког приступа или оштећења критичних компоненти;
4) физичка заштита информатичких ресурса који се налазе у подручним одељењима обезбеђује се у складу са условима прописаним у ставу 2 овог члана и онемогућава неовлашћени приступ кључној опреми, ради спречавања видљивости поверљивих информација и активности споља;
5) физичка заштита се мора планирати и за случајеве злонамерних напада, природних катастрофа или несрећа;
6) медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

Води се и одговарајућа евиденција о уласку у заштићену зону.

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

Члан 18

Улаз у простор у коме се налази део ИКТ опреме (сервер сала) дозвољен је само оператерима ИКТ система и запосленима на пословима ИКТ система.

Осим дежурног оператера, приступ сервер сали могу имати и трећа лица ради инсталације и сервисирања одређених ресурса ИКТ система, уз присуство надлежног лица.

Приступ сервер сали може имати и запослени на пословима одржавања.

У овом простору се редовно врши контрола система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, електронску комуникацију.

Опрема мора бити заштићена од влаге, пожара, прашине, атмосферских и електромагнетних утицаја.

Сервери и активна мрежна опрема *(switch, modem, router, firewall)* морају стално бити прикључени на уређаје за непрекидно напајање.

Ако се опрема износи ради сервисирања, поред одобрења добијеног од стране надлежног лица, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив овлашћеног сервиса, име и презиме овлашћеног лица сервиса.

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

Све осетљиве и поверљиве информације се штите у складу са Правилником о заштити статистичких података у Заводу.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19

Коришћење ресурса се надгледа, подешава и пројектује у складу са захтеваним капацитетима у наредном периоду, како би се осигурале захтеване перформансе система. 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 с тим, планирају, односно предлажу одговарајуће мере.

Пре увођења у продукцију новог софтвера неопходно је направити копију – архиву постојећих података, ради 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 корисника ИКТ система. 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 систему, 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.

15. Заштита података и средстава за обраду података од злонамерног софтвера

Члан 20

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете ресурсе ИКТ система. Заштита података и средстава за обраду података од злонамерног софтвера се заснива на превенцији и откривању злонамерног софтвера, отклањању штете, као и на одговарајућим контролама приступа систему и управљања захтеваним и потребним променама.

Заштита од злонамерног софтвера на мрежи спроводи се ради заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (USB меморија, CD итд.).

Завод одређује и примењује контроле откривања, спречавања и опоравка ИКТ система, ради заштите од злонамерног софтвера.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефиниција.

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

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

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

Ради сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

- електронска пошта са прилозима се не сме отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;
- забрањено је коришћење електронске поште у приватне сврхе;
- не смеју се користити приватни налози електронске поште у пословне сврхе.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави надлежној организационој јединици.

16. Заштита од губитка података

Члан 21

Заштита од губитка података у Заводу врши се израдом резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

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

Прављење заштитних копија и заштита од губитка података обавља се у складу са Правилником о архивирању и бекапу електронских података у Заводу.

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

Члан 22

У ИКТ систему Завода формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу информација, који се морају чувати и редовно преиспитивати.

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

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 23

У ИКТ систему Завода може да се инсталира само софтвер одобрен од стране овлашћене службе. Завод спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система.

Инсталацију и подешавање софтвера може да изврши само лице које има овлашћење за то, као 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.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24

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

Анализа дневника активности (*activitylog*, *history*, *securitylog*, *transactionlog* и др.) врши се ради идентификације потенцијалних слабости ИКТ система, а спроводи је надлежна организациона јединица.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, неопходно је извршити подешавања, односно инсталирање софтвера који ће отклонити уочене слабости, као и онемогућавање неовлашћеног инсталирања софтвера који може довести до угрожавања безбедности ИКТ система.

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

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

Члан 25

Ревизија ИКТ система мора се вршити тако да има што мањи утицај на пословне процесе корисника ИКТ система. Уколико то није могуће извести у току радног времена због ометања пословног процеса, врши се ван радног времена, уз претходно добијену сагласност одговорног лица.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 26

Мрежне услуге обухватају обезбеђивање прикључака, услуге на приватним мрежама и мреже са допуњеним функцијама, решења за управљање безбедношћу информација, као што су заштитне преграде и системи за откривање упада.

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

У мрежама су међусобно раздвојене групе информационих услуга, корисника и информациони системи, а мрежни оператер је одговоран за управљање мрежом и благовремено предузимање мера ради отклањања евентуалних неправилности.

Заштита података се врши и постављањем комуникационих каблова и каблова за напајање у зиду или каналицама тако да се онемогући неовлашћен приступ и могуће оштећење комуникационих каблова и каблова за напајање.

22. Безбедност података који се преносе унутар Завода, као и између Завода и лица ван Завода

Члан 27

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

Употреба електронске поште мора бити у складу са правилима поступка, сигурна и у складу са позитивним прописима и пословном праксом.

Електронска пошта се може користити искључиво за пословне потребе. Сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

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

Споразуми о поверљивости или неоткривању информација обавезују потписнике да их штите, користе и објављују на одговоран и ауторизован начин.

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

Члан 28

Завод је у обавези да обезбеди безбедност информација у току животног циклуса ИКТ система који укључује фазе његовог конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе.

Питање безбедности се анализира у раним фазама пројектовања информационог система, јер такво разматрање доводи до ефикаснијих и рационалнијих решења.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система, надлежна служба води потребну евиденцију.

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

У захтев за набавку новог информационог система или за побољшање постојећег информационог система морају бити укључени захтеви који се односе на безбедност информација и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

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

У уговору о куповини информационих добара дефинишу се захтеви безбедности.

За технички надзор над реализацијом уговорених обавеза од стране трећих лица, задужена је надлежна организациона јединица.

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

Члан 29

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама.

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

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

Тестирање и испитивање ИКТ система врши надлежна организациона јединица.

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

Члан 30

Уговори које закључује Завод са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација морају садржати уговорну одредбу о заштити и чувању поверљивих информација, података и документације.

Пружаоци услуга имају право на приступ само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ.

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

Контролу, приступ и надзор над поштовањем уговорених обавеза од стране пружаоца услуга – трећих лица, посебно у области која регулише безбедност ресурса ИКТ система, обавља надлежна организациона јединица.

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

Члан 31

Завод нема склопљен уговор са трећим лицима за пружање услуга информационе безбедности.

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

Члан 32

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, сваки корисник ИКТ система је дужан да одмах обавести надлежног

руководиоца ИКТ система и предузме мере ради заштите ресурса ИКТ система и спречавања настанка штете.

Надлежна организациона јединица води евиденцију о свим инцидентима, као и пријавама инцидената, на основу којих се против корисника ИКТ система који је изазвао инцидент, може водити дисциплински, прекршајни или кривични поступак.

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

Уколико је реч о инциденту који је дефинисан Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, Завод је дужан да обавештење о инциденту достави министарству надлежном за информациону безбедност, Народној банци Србије и регулаторном телу за електронске комуникације.

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33

Завод примењује мере које обезбеђују континуитет обављања послова у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

Сви запослени су дужни да спроведу прописане процедуре неопходне за функционисање ИКТ система у таквим условима.

III. ИЗМЕНА ПРАВИЛНИКА О БЕЗБЕДНОСТИ

Члан 34

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, извршиће се потребне измене овог Правилника о безбедности, а с циљем његовог унапређења.

IV. ПРОВЕРА ИКТ СИСТЕМА

Члан 35

Обавеза Завода је да врши проверу ИКТ система најмање једном годишње ради провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности, усклађених са Правилником о безбедности, мерама заштите прописаним Законом о информационој безбедности и Уредбом о мерама заштите, о чему ће се сачинити посебан извештај.

V. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 36

Овај Правилник о безбедности ступа на снагу наредног дана од дана његовог објављивања на огласној табли Завода.

У Београду, 26.септембра 2017. године

Директор

Др Миладин Ковачевић