На основу члана 135. Закона о раду („Службени гласник РС”, број 24/05, 61/05, 54/09, 32/13, 75/14 и 13/17 – одлука УС), а везано за члан 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16), и члан 2. Уредбе о ближем садржају акта 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 („Сл. Гласник РС“, бр. 94/2016), директор Фонда солидарности дана 16.06.2017.године, доноси

ПРАВИЛНИК
о безбедности информационо - комуникационог система Фонда солидарности

I. Уводне одредбе

Члан 1.

Овим правилником се утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система Фонда солидарности, а у складу са Законом о информационој безбедности и Уредбом о ближем садржају правилника о безбедности информационо-комуникационих система од посебног значаја, начин провере информационо-комуникационих система од посебног значаја и садржај извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС“, бр. 94/2016).

Члан 2.

Доношењем правилника о безбедности ИКТ система Фонда солидарности доприноси се смањењу могућности ризика од инцидената и нарушавања интегритета, као и доприносу подизања свести код запослених у Фонду солидарности о ризицима и опасностима које су везане за коришћење информационих технологија.

Члан 3.

Мере прописане овим правилником се односе на све организационе структуре Фонда солидарности, на све запослене (кориснике информатичких ресурса), као и на трећа лица која користе информатичке ресурсе Фонда солидарности.

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог (корисника информатичких ресурса) Фонда солидарности.

За праћење примене овог правилника обавезује се систем администратор.

Члан 4.

Поједини термини у смислу овог правилника имају следеће значење:

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

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

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

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

(4) организациону структуру путем које се управља 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, када је предвиђено и под контролом овлашћених лица;

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

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

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* је податак који је, у складу са прописима о тајности података, 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 или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
20) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
21) VPN (Virtual Private Network)-је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
22) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
23) Backup је резервна копија података;
24) Download је трансфер података са централног рачунара или web презентације на локални рачунар;
25) UPS (Uninterruptible power supply*)* је уређај за непрекидно напајање електричном енергијом;
26) Freeware је бесплатан софтвер;
27) Opensource софтвер отвореног кода;
28) Firewall је „заштитни зид“ односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
29) USB или флеш меморија је спољшњи медијум за складиштење података;
30) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;
31) DVD је оптички диск високог капацитета који се користи као медијум 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 Фонда солидарности, а посебно у оквиру пружања услуга другим лицима.

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

Члан 6.

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

За контролу и надзор над обављањем послова запослених (корисника), у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Фонда солидарности надлежан је систем администратор, у складу са систематизацијом радних места у Фонду солидарности.

Члан 7.

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 онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Фонда солидарности, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента систем администратор обавештава шефа одсека за финансијско-књиговодствене и опште послове, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 8.

Запослени (корисници), путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ Интернету путем рутера са ограниченим MAC адресама, а које су унете у листу софтвера који се користи за контролу приступа, али не и деловима мреже кроз коју се обавља службена комуникација.

Запослени (корисници ресурса ИКТ система), могу путем мобилних уређаја који су подешени од стране систем администратора да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности (коришћење електронске поште), а на основу писане сагласности шефа одсека за финансијско-књиговодствене и опште послове.

Запосленом (кориснику), забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.)

Евиденцију приватних уређаја са којих ће бити омогућен приступ само оним деловима ИКТ система који им омогућавају обављање радних задатака води систем администратор, а по одобрењу шефа одсека за финансијско-књиговодствене и опште послове.

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

Члан 9.

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места.
Систем администратор је дужан да сваког новозапосленог (корисника ИКТ ресурса) упозна са одговорностима и правилима коришћења ИКТ ресурса Фонда солидарности, као и да води евиденцију о изјавама новозапослених (корисника) да су упознати са правилима коришћења ИКТ ресурса.

Свако коришћење ИКТ ресурса Фонда солидарности од стране запосленог (корисника), ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

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

Члан 10.

У случају промене послова, односно надлежности запосленог (корисника), систем администратор ће извршити промену привилегија које је запослени (корисник) имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

У случају престанка радног ангажовања запосленог (корисника), кориснички налог се укида.

О престанку радног односа или радног ангажовања, као и промени радног места, саветник за опште-правне послове, у сарадњи са непосредним руководиоцем, је дужана да обавести систем администратора ради укидања, односно измене приступних привилегија тог запосленог (корисника).

Корисник ИКТ ресурса, након престанка радног ангажовања у Фонду солидарности, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра Фонда солидарности су сви ресурси који садрже пословне информације Фонда солидарности, 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 који се односе на ИКТ систем и сл.

Евиденцију о информационим добрима води систем администратор, 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

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

Члан 12.

Подаци који се налазе у ИКТ систему представљају пословну тајну и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. Гласник РС“, бр. 53/2011).

7. Заштита носача података

Члан 13.

Подаци и документи 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 шефа одсека за финансијско-књиговодствене и опште послове.

Подаци и документи могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених (корисника).

Евиденцију носача на којима су снимљени подаци води систем администратор и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

Систем администратор ће, такође, успоставити организацију приступа и рада са подацима.

8. Ограничење приступа подацима и средствима за обраду података

Члан 14.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени (корисник) има.
Запослени који има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

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

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

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

Право приступа имају само запослени (корисници) који имају администраторске или корисничке налоге.
Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.
Администраторски налог могу да користе само запослени на пословима: систем администратора, референта логистике и директора Фонда солидарности.
Адинистраторски налог за управљање базом података могу да користе само запослени на пословима: систем администратора, референта логистике и директора Фонда солидарности.

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

Кориснички налог додељује администратор, на основу захтева запосленог задуженог за управљање људским ресурсима (саветник за опште-правне послове) у сарадњи са директором Фонда солидарности, и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима, а у складу са потребама обављања пословних задатака од стране запосленог (корисника).

Администратор 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 директора Фонда солидарности.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 16.

Кориснички налог се састоји од корисничког имена и лозинке.

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

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке.

Ако запослени (корисник) посумња да је друго лице открило његову лозинку, дужан је да исту одмах измени.

Запослени (корисник) је дужан да мења лозинку најмање једном у шест месеци.

Иста лозинка се не сме понављати у временском периоду од годину дана.

Неовлашћено уступање корисничког налога другом лицу подлеже дисциплинској одговорности.

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

Члан 17.

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

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

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

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, мрежна или комуникациона опрема ИКТ система, организује се као административна зона (сервер соба), која испуњава стандарде противпожарне заштите, поседује константно напајање електричном енергијом, адекватну климатизацију, као и меру заштите услед нестанка електричне енергије (UPS).

Сервер соба је обезбеђена механичком бравом и видно означена.

Приступ сервер соби поред лица која су задужена за одржавање ИКТ система у Фонду солидарности, могу имати и лица запослена у Републичком заводу за статистику.

Административну зону (сервер собу) заједнички деле Фонд солидарности и Републички завод за статистику.

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

Члан 19.

Улаз у сервер собу у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу шефа одсека за финансијско-књиговодствене и опште послове и уз присуство систем администратора, као и запосленог/е на пословима одржавања хигијене.

Приступ административној зони могу имати искључиво лица која се предходно евидентирају код обезбеђења зграде.

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

Сервери морају стално бити прикључени на уређаје за непрекидно напајање – UPS.

У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, а току радног времена, 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 шефа одсека за финансијско-књиговодствене и опште послове.

У случају изношења опреме ради селидбе, директора Фонда солидарности ће одредити услове пресељења.

У случају изношења опреме ради сервисирања, неопходно је одобрење секретара Фонда солидарности.

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

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 20.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим, планирају, односно предлажу шефу одсека за финансијско-књиговодствене и опште послове 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.

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

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 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, e-mail (ом), зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

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

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

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

Приликом коришћења интернета треба избегавати сумњиве WEB странице, с' обзиром да то може проузроковати одређене проблеме (неприметно инсталирање шпијунских програма и слично).

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

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" WEB страницама 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, audio/video streaming и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

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.

Базе података обавезно се архивирају на преносиве медије (CDROM, DVD, USB, „strimer" трака, екстерни хард диск), најмање једном дневно, недељно, месечно и годишње, за потребе обнове базе података.

Остали фајлови (документи) се архивирају најмање једном недељно, месечно и годишње.

Дневно копирање (архивирање) се врши сваки радни дан у недељи, при крају радног времена.

Недељно копирање (архивирање) се врши последњег радног дана у недељи, при крају радног времена.

Сваки примерак преносног информатичког медија са копијама (архивама), мора бити означен заводним бројем.

Дневне и недељне копије (архиве) се чувају у просторији која је физички обезбеђена.

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

Члан 23.

О активностима администратора и запослених (корисника) воде се дневници активности (activitylog, history, securitylog, transactionlog и др).

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 Фонда солидарности или Управе за заједничке послове, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само систем администратор, односно запослени (корисник) који има овлашћење за то.

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

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

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, систем администратор је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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 запослених (корисника). Уколико то није могуће у радно време, онда се врши након завршетка радног времена запослених (корисника), чији би пословни процес био ометан, уз претходну сагласност шефа одсека за финансијско-књиговодствене и опште послове.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 27.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, router, firewall) се мора налазити у rack орману.

Систем администратор је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

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

Члан 28.

Преносиви медији (екстерни хард дискови) који садрже податке морају да буду прописно обележени и потпсани.

Преносиви медији пре стављања ван употребе морају бити физички уништени.

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

Члан 29.

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

Систем администратор је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

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

Члан 30.

За потребе тестирања ИКТ система односно делова система, систем администратор може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

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

Члан 31.

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

Систем администратор је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

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

Члан 32.

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

За пружање услуга информационе безбедности Фонду солидарности задужена је Управа за заједничке послове.

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 систем администратора.

По пријему пријаве, систем администратор је дужан да одмах обавести шефа одсека за финансијско-књиговодствене и опште послове и предузме мере у циљу заштите ресурса ИКТ система.

Систем администратор води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

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 Фонда солидарности, систем администратор је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију (зграда СИВ-а III – архива Фонда солидарности, Омладинских бригада 1).

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује систем администратор, и то у три примерка, од којих се један налази код њега, други код запосленог надлежног за послове одбране и ванредне ситуације, а трећи примерак код шефа одсека за финансијско-књиговодствене и опште послове.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди шеф одсека за финансијско-књиговодствене и опште послове.

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

III. Измена правилника о безбедности

Члан 35.

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, систем администратор је дужан да обавести шефа одсека за финансијско-књиговодствене и опште послове, како би он могао да приступи 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.

IV. Провера ИКТ система

Члан 36.

Проверу ИКТ система врши систем администратор.

Проверу ИКТ система се вршити последњег месеца у години.

Провера се врши тако што се:
1) проверава усклађеност правилника о безбедности ИКТ система, узимајући у обзир и правилнике на која 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 шефу одсека за финансијско-књиговодствене и опште послове.

V. Садржај извештаја о провери ИКТ система

Члан 37.

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 правилником 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.

VI. Прелазне и завршне одредбе

Члан 38.

Овај правилник ступа на снагу наредног дана од дана објављивања на огласној табли и интернет страници Фонда солидарности.

Број: 110-00-1/2017-01
Београд, 16.06. 2017.године.

ДИРЕКТОР

Јаблан Обрадовић