ИНСТИТУТ ЗА НУКЛЕАРНЕ НАУКЕ «ВИНЧА»
ИНСТИТУТ ОД НАЦИОНАЛНОГ ЗНАЧАЈА ЗА РЕПУБЛИКУ СРБИЈУ
УНИВЕРЗИТЕТ У БЕОГРАДУ
Деловодни број: 011-10/2020-000
Датум: 09.07.2020. године

На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16, 94/2017 и 77/2019), члана 2. 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 63. став 1. тачка 7) Закона о науци и истраживањима (Сл. Гл. Републике Србије 49/2019) и члана 36. Статута Института за нуклеарне науке „Винча", в.д. директора Института за нуклеарне науке" Винча" – Института од националног значаја за Републику Србију – Универзитета у Београду, ул. Мике Петровића Аласа бр. 12-14, Београд – Винча (у даљем тексту: Институт), дана 09.07.2020. године доноси

ПРАВИЛНИК

о безбедности информационо-комуникационих система у Институту за нуклеарне науке " Винча"

Уводне одредбе

Члан 1.

Овим правилником, ближе се дефинишу и утврђују мере заштите, информационо - комуникационих система, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења, дужности и одговорности запослених и уговором ангажованих лица у Институту (у даљем тексту: ***корисника информатичких ресурса***), у Институту.

Члан 2.

Циљеви доношења овог Правилника су:

1. допринос подизању нивоа опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
2. минимизација безбедоносних ризика;
3. допринос развоју одговарајућих безбедоносних апликација и обезбеђивања перманентне контроле свих компонената информационо-комуникационих система (у даљем тексту: **ИКТ систем**).

Члан 3.

Мере прописане овим правилником обавезујуће су за све организационе јединице Института , односно за сва запослена и уговором ангажована лица ван радног односа у Институту (у даљем тексту: кориснике информатичких ресурса) и трећа лица.

Непоштовање овог правилника представља повреду радне обавезе и непоштовање радне дисциплине, корисника информатичких ресурса Института за нуклеарне науке "Винча".

За праћење примене овог правилника надлежна је Служба за одржавање рачунара и рачунарске мреже (у даљем тексту: **Служба за ИКТ**).

Члан 4.

Поједини изрази употребљени у овом правилнику имају следеће значење:

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

1.1 електронске комуникационе мреже у смислу закона који уређује електронске комуникације;

1.2 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;

1.3 податке који се похрањују, обрађују, претражују или преносе помоћу средстава из 1.1 и 1.2 ове тачке, а у сврху њихове употребе. заштите или одржавања;

1.4 организациону структуру (систем администратори, инжењери различитих информатичких специјалности, техничари,) путем које се управља ИКТ системом (одржавање и развој);

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

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 код, 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 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-а на локални рачунар;

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

26. ***Freeware*** је бесплатан софтвер;

27. ***Open source*** је софтвер отвореног кода;

28. ***Firewall*** је „заштитни зид" односносистем 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 користио као медијум за снимање података али и даље је у употреби;

31. ***DVD*** је оптички диск високог капацитета који се користио као медијум за складиштење података али и даље је у употреби;

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

Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Института, односно заштита података садржаних у ИКТ систему од:

- неовлашћеног приступа,

- модификације,
- коришћења без овлашћења и без евиденције,
- деструкције или
- уништења

на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Организациона структура, са утврђеним пословима и одговорностима корисника информатичких ресурса, којом се остварује управљање информационом безбедношћу

Члан 6.

Сваки корисник информатичких 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 корисника информатичких ресурса, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Института, надлежна је Служба за ИКТ, односно сви запослени са администраторским овлашћењима који су задужени за одржавање информатичких ресурса.

Члан 7.

Послови из области безбедности су:

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

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

Безбедност рада на даљину и употреба уређаја

Члан 8.

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

Корисници информатичких ресурса ИКТ система, могу путем уређаја,

који су у власништву Института и који су подешени од стране запослених из Одељења за ИКТ, односно администратора задужених за информатичку подршку (у даљем тексту: Администратори задужени за ИП), на основу писане сагласности овлашћеног лица, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности.

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

Приступ ресурсима ИКТ система Института са удаљених локација, од стране корисника информатичких ресурса, у циљу обављања радних задатака, омогућен је путем заштићене „*WireLess*" интернет конекције.

Корисницима информатичких ресурса, забрањена је самостална инсталација софтвера и подешавање уређаја, као и давање уређаја другим неовлашћеним лицима, обзиром да се исто има сматрати повредом радне обавезе и непоштовањем радне дисциплине.

Запослени из Службе за ИКТ, односно администратори мреже свакодневно контролишу приступ ресурсима ИКТ система и проверавају да ли је остварен приступ са непознатих уређаја (са непознатих „*MAC*" адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава руководилац Службе за ИКТ. Непозната „*MAC*" адреса се уноси у "block" листу софтвера који се користи за контролу приступа.

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

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

Изузетно од става 8. овог члана, у случају неопходних и хитних послова могу се одобрити права приступа ИКТ систему трећем лицу по писаном налогу директора Института или другог овлашћеног лица, (email, sms, писани акт).

По завршетку посл ће бити сачињен записник о оствареном приступу.

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

Евиденцију приватних уређаја са којих ће бити омогућен приступ воде запослени из Службе за ИКТ, а по одобреној процедури.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система, морају бити подешени-сертификовани од стране запослених из Службе за ИКТ и могу се користити само за обављање послова у надлежности или делокругу рада корисника информатичких ресурса.

Запослени из Службе за ИКТ су дужни да пре предаје уређаја овлашћеном сервису, уколико квар није такве врсте да то онемогућава, уради *„BACKUP"* података који се налазе у мобилном уређају, а потом их обришу из уређаја и по повратку из сервиса поново врате податке у уређај.

Обезбеђивање да корисници информатичких ресурса ИКТ система разумеју своју одговорност

Члан 9.

Директор Института, помоћници директора Института, директори и руководиоци организационих јединица Института, су дужни да сваког новог корисника информатичких ресурса ИКТ система пошаљу на кратку обуку у Службу за ИКТ где ће бити упознати са одговорностима и правилима коришћења ИКТ ресурса.

Свако коришћење ИКТ ресурса Института за нуклеарне науке "Винча" од стране корисника информатичких ресурса, ван додељених овлашћења, има се сматрати повредом радне обавезе и непоштовањем радне дисциплине.

Заштита од ризика који настају при промени радног места или престанка радног односа, односно престанка ангажовања лица ван радног односа запослених у Служби за ИКТ

Члан 10.

У случају промене радног места, односно надлежности запосленог, то јест лица ангажованог ван радног односа, запослени са администраторским овлашћењима у Служби за ИКТ, ће извршити промену привилегија које је запослени или лица ангажовано ван радног односа имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

У случају престанка радног односа, односно престанка ангажовања лица ван радног односа кориснички налог се укида.

За време и по престанку радног односа или престанку ангажовања лица ван радног односа, као и промени радног места запосленог, непосредни руководилац је дужан да електронским путем обавести Службу за ИКТ ради укидања односно измене приступних привилегија именованог корисника информатичких ресурса.

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

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра Института су сви ресурси који садрже пословне информације Института у електронском облику или служе за приступ корисника информатичких ресурса ИКТ систему, укључујући:

- све електронске записе,
- рачунарску опрему,
- комуникациону опрему,
- уређаје,
- базе података,
- пословне апликације и слично

путем којих се врши израда, обрада, чување, пренос или брисање података у ИКТ систему.

Евиденцију о информационим добрима (основна средства, алати, прибор, материјал и документација), поред Самосталног референта основних средстава, односно запослених у Одељењу Књиговодства, води и администратор из Службе за ИКТ, у папирној или електронској форми.

Предмет заштите су:

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

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

Члан 12.

Подаци који се налазе у ИКТ систему представљају тајну и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима.

Детаљан опис информација, носачима информација и доступности података који су означени одређеним степеном тајности, одређени су Одлуком о одређивању тајних података у Институту и Каталогом докумената, података и информација који треба да буду означени степеном тајности „ПОВЕРЉИВО“ или „ИНТЕРНО“.

Заштита носача података

Члан 13.

Руководилац Службе за ИКТ успоставиће организацију приступа и рада са подацима, посебно онима који буду означени степеном тајности у складу са Законом о тајности података, тако да:

1. подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само корисници информатичких ресурса којима је издат сертификат за приступ тајним подацима;
2. подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, *USB, CD, DVD, ext HDD*), само од стране корисника информатичких ресурса којима је издат сертификат за приступ тајним подацима, а по налогу руководиоца Службе за ИКТ.

Евиденцију носача на којима су снимљени подаци, воде корисници информатичких ресурса којима је издат сертификат за приступ тајним подацима, а по налогу руководиоца Службе за ИКТ 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. руководилац Службе за ИКТ ће одредити одговорну особу и начин транспорта.

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

Ограничење приступа подацима и средствима за обраду података

Члан 14.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном привилегијом коју корисници информатичких ресурса поседују.

Корисници информатичких ресурса који поседују администраторски налог, имају права приступа свим ресурсима ИКТ система (софтверским, хардверским, мрежи и мрежним ресурсима) у циљу:

- инсталације,
- одржавања,
- подешавања,
- провера односно тестирању и
- управљања ресурсима ИКТ система.

Корисници информатичких ресурса могу да користе само свој кориснички налог који су добили од администратора и не смеју да омогућавају другом лицу коришћење њиховог корисничког налога.

Корисници информатичких ресурса који на било који начин злоупотребе корисничка права, односно ресурсе ИКТ система, подлежу кривичној, материјалној и одговорности по основу повреде радне обавезе и непоштовања радне дисциплине.

Корисници информатичких ресурса су дужни да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система и то да:

1. користе информатичке ресурсе искључиво у пословне сврхе;
2. прихвате да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Института и да могу бити предмет надгледања и прегледања од овлашћених лица;
3. поступају са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. безбедно чувају своје лозинке, односно да их не одају другим лицима;
5. мењају лозинке сагласно утврђеним правилима;
6. пре сваког удаљавања од радне станице, одјаве се са система, односно закључају радну станицу;
7. захтев за инсталацију софтвера или хардвера подносе у писаној

форми, одобрен од стране непосредног руководиоца, Служби за ИКТ;
8. обезбеде сигурност података у складу са важећим прописима;
9. приступају информатичким ресурсима само на основу експлицитно додељених корисничких права;
10. не смеју да заустављају рад или бришу антивирусни програм, мењају његове подешене опције, нити да неовлашћено инсталирају други антивирусни програм;
11. на радној станици не смеју да складиште садржај који не служи у пословне сврхе;
12. израђују заштитне копије података у складу са прописаним процедурама;
13. користе интернет и електронску пошту у складу са прописаним правилима;
14. прихвате да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
15. прихвате да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
16. прихвате да технике сигурности (антивирус програми, *„firewall*", системи за детекцију упада, средства за шифрирање. средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;
17. не смеју да инсталирају, модификују, искључују из рада или бришу заштитни, системски или апликативни софтвер.

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

Члан 15.

Администраторски налози свих пословних апликација, сервера база података и системских апликација за управљање мрежном опремом и уређајима за складиштење података чувају се у затвореним, непровидним ковертама са отиском службеног печата, у каси код директора/руководиоца организационе јединице.

Право коришћења администраторског налога имају само Корисници информатичких ресурса са администраторским овлашћењима за потребе информатичких интервенција.

Након сваког отварања коверте и коришћења администраторског налога од стране Корисника информатичких ресурса са администраторским овлашћењима, директор/руководилац организационе јединице је дужан да промени лозинку администраторског налога.

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

Администраторска овлашћења могу добити само лица која су задужена за одржавање информатичких ресурса, уз претходну сагласност руководиоца Службе за ИКТ.

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 се врши аутентификација-провера идентитета и ауторизација - провера права приступа, односно права коришћења ресурса ИКТ система од стране Корисника информатичких ресурса.

Запослени са администраторским овлашћењима, на основу прецизног писаног захтева непосредног руководиоца, додељује кориснику информационог ресурса корисничко име, лозинку, привилегије и налог за електронску пошту.

Запослени са администраторским овлашћењима воде евиденцију о корисничким налозима, проверавају њихово коришћење, мењају права приступа и укидају корисничке налоге на основу захтева непосредног руководиоца.

Запосленима у Службе за ИКТ са администраторским овлашћењима забрањена је злоупотреба података којима имају приступ.

Злоупотребу података врши лице које достави информацију трећим лицима или учини јавно доступним податке којима има приступ.

Запосленима у Службе за ИКТ са администраторским овлашћењима који злоупотребе своја овлашћења подлежу кривичној, материјалној и одговорности по основу повреде радне обавезе и непоштовања радне дисциплине.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 16.

Кориснички налог се састоји од корисничког имена и лозинке.

Карактеристике довољно сигурних лозинки које се морају користити су дефинисане Правилником о употреби рачунарско-комуникационих ресурса на мрежи VincaNet-а.

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

Корисници информатичких ресурса су дужни да мењају лозинку најмање једном у шест месеци.

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

Кориснички налог може да се се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр. лична карта са чипом и уписаним сертификатом).

Неовлашћено уступање корисничког налога другом лицу има се сматрати повредом радне обавезе и непоштовањем радне дисциплине.

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

Члан 17.

Приступ ресурсима ИКТ система Института не захтева посебну криптозаштиту.

За приступ ресурсима ИКТ система који се односе на послове одбране, односно, за које је надлежно министарство прописало коришћење криптозаштите, посебним правилником ће бити дефинисана употреба одговарајућих мера криптозаштите узимајући у обзир осетљивост информација које треба да се штите, пословне процесе који се спроводе, ниво захтеване заштите, имплементацију примењених криптографских техника и управљање криптографским кључевима.

Корисници информатичких ресурса користе квалификоване електронске сертификате за електронско потписивање докумената, као и аутентификацију и ауторизацију приступа појединим апликацијама.

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

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

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

Члан 18

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

Простор мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода и у њему треба да буде одговарајућа температура.

Евиденцију о уласку у ову зону воде запослени у Служби за ИКТ.

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

Члан 19.

Улаз у простор у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система, односно запосленима на пословима одржавања ИКТ система.

Осим администратора система и запослених на пословима одржавања ИКТ система, приступ административној зони могу имати и трећа лица

у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу руководиоца Службе за ИКТ, и уз присуство заспосленог из Службе за ИКТ.

Приступ административној зони може имати и лице које обавља послове одржавања хигијене уз присуство запосленог из Службе за ИКТ.

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

Прозори и врата на овој просторији морају увек бити затворени.

Сервери и активна мрежна опрема (*switch, modem, router, firewall*), морају стално бити прикључени на уређаје за непрекидно напајање - *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 слично) може изнети и без одобрења руководиоца организационе јединице.

У случају изношења опреме ради селидбе или сервисирања, неопходно је одобрење руководиоца Службе за ИКТ.

Ако се опрема износи ради сервисирања, потребно је сачинити и Ревер у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера и име и презиме запосленог који је опрему предао и њехови потписи.

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

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. У складу са напред наведеним, планирају и предлажу руководиоцу Службе за ИКТ 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 мора се вршити на начин који не омета оперативни рад Корисника информатичких ресурса.

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

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

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

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 21.

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

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

Сваке среде у току радног времена је потребно оставити укључене све радне станице ради антивирус скенирања.

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

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

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

У циљу заштите, односно упада у ИКТ систем Института са интернета, Служба за ИКТ је дужна да одржава систем за спречавање упада.

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

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

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

Информацију о инциденту Корисник информатичких ресурса је дужан да одмах проследи непосредном руководиоцу и запосленима са администраторским овлашћењима у Служби за ИКТ.

Строго је забрањено гледање филмова и играње игрица на рачунарима и посета *WEB* страницама које садрже непримерен садржај, као и самовољно преузимање истих са интернета.

Недозвољена употреба интернета обухвата:

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

Корисници који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже чине повреду радне обавезе и непоштовања радне дисциплине.

Заштита од губитка података

Члан 22.

Израда резервних копија база података, фолдера, фајлова-докумената, врши Корисник на преносиве медије (*CD ROM. DVD, USB, „strimer*" трака, ext *HDD* или *SSD*) једном дневно, недељно, месечно и годишње, за потребе обнове базе података у зависности од значаја податка, што ће бити дефинисано Политиком заштите и архивирања података на нивоу Института.

Сваки примерак годишње копије/архиве база података, фолдера, фајлова-докумената, чува се у роковима који ће бити дефинисани Политиком заштите и архивирања података на нивоу Института.

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

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

од пожара.

Годишње копије-архиве се израђују у два примерка, од којих се један чува у просторији у којој се чувају дневне, недељне и месечне копије-архиве а други примерак се одлаже на другој безбедној локацији.

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

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

Члан 23.

О активностима администратора и запослених односно корисника воде се дневници активности (*activity_log, history_log, security_log. Transaction_log* и друго).

Сваког последњег радног дана у недељи датотеке у којима се налази дневник активности се архивирају по процедури за израду копија - архива осталих података у ИКТ систему, у складу са чланом 22. овог правилника.

Систем за контролу и дојаву о грешкама и неовлашћеним активностима, мора бити подешен тако да одмах обавештава запослене са администраторским овлашћењима, руководиоца организационе јединице надлежне за послове ИКТ и руководиоца Службе за ИКТ, о свим нерегуларним активностима запослених односно корисника, о покушајима упада и упадима у систем.

Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Института, односно *Freeware* и *OpenSource* верзије.

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

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

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

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

Запослени са администраторским овлашћењима у Службе за ИКТ најмање једном месечно, а по потреби и чешће врши анализу дневника активности (*activity_log, history_log, security_og, transaction_log* и друго), у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, запослени са администраторским овлашћењима, дужни су да одмах изврше подешавања, односно инсталацију софтвера који ће отклонити уочене слабости.

Запослени са администраторским овлашћењима треба да подешавањем корисничких полиса, онемогуће неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

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 Корисника информатичких ресурса.

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

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 закључаном *rack* орману.

Запослени са администраторским овлашћењима у Служби за ИКТ су дужни да стално врше контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коју могу да користе посетиоци објеката у надлежности Института мора бити одвојена од интерне мреже кроз коју се врши размена службених података.

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

Члан 28.

Размена података са државним органима, органима локалних

самоуправа, академском заједницом, правним и физичким лицима се врши у складу са важећим прописима и унапред дефинисаним и потписаним уговорима, споразумима и протоколима.

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

Члан 29.

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

Запослени из Службе за ИКТ су задужени за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

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

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

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

Члан 30.

За потребе тестирања ИКТ система односно делова система запослени из Службе за ИКТ могу користити податке који нису осетљиви, које штите, чувају и контролишу на одговарајући начин.

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

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 31

Трећа лица-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.

Запослени из Службе за ИКТ су одговорни за контролу приступа и надзор над извршењем уговорених обавеза. као и за поштовање одредби овог правилника којима су такве активности дефинисане.

Одржавање уговореног нивоа информационе безбедности и

пружених услуга у складу са условима који су уговорени са пружаоцем услуга

Члан 32.

Запослени из Службе за ИКТ су одговорни за надзор над поштовањем уговорених обавеза од стране трећих лица-пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система.

У случају непоштовања уговорених обавеза запослени из Службе за ИКТ су дужни да одмах обавесте свог руководиоца и по потреби директора Института, како би он могао да предузме мере у циљу отклањања неправилности.

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

Члан 33.

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

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

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података: листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, руководиоц Службе за ИКТ дужан је да поред директора Института обавести и надлежни орган дефинисан 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.

Запослени у Служби за ИКТ воде евиденцију о свим инцидентима, као и пријавама инцидената, у складу са наведеном уредбом, на основу које, против одговорног лица, могу да се воде поступак утврђивања радне обавезе или непоштовања радне дисциплине, прекршајни или кривични поступци.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 34.

У случају ванредних околности које могу да доведу до измештања ИКТ система из просторија Института, запослени са администраторским овлашћењима у Служби за ИКТ су дужни да у најкраћем року пренесу делове ИКТ система (или обезбеде функционисање редундантних компоненти на резервној локацији уколико постоје) неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са општим актима Института.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује Служба за ИКТ, и то у два примерка, од којих се један налази код руководиоца Службе за ИКТ, други примерак код директора Института.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди директор Института.

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.

Провера ИКТ система

Члан 35.

Проверу ИКТ система врши запослени са администраторским овлашћењима у Службе за ИКТ.

Проверу ИКТ система може вршити и лице изабрано у складу са законом којим се уређује поступак јавних набавки. Провера ће се вршити прве недеље седмог месеца у години.

Провера се врши тако што се:

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

О извршеној провери сачињава се Извештај, који се доставља руководиоцу Службе за ИКТ, који га по портеби даље прослеђује.

Садржај извештаја о провери ИКТ система

Члан 36.

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 информационо-комуникационих система у Институту, 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;
потпис одговорног лица које је спровело проверу ИКТ система.

Прелазне и завршне одредбе

Члан 37.

У случају настанка промена које могу наступити услед техничко – технолошких, кадровских и организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, руководилац Службе за ИКТ је дужан да о томе обавести директора Института, ради издавања налога да се приступи измени овог правилника.

Члан 38.

Одлука о одређивању тајних података у Институту и Каталог докумената, података и информација који треба да буду означени степеном тајности „ПОВЕРЉИВО" или „ИНТЕРНО", биће донети у року од 6 месеци од дана ступања на снагу овог Правилника.

Члан 39.

Овај Правилник ступа на снагу осмог дана од дана његовог доношења и објављивања на огласној табли и Web сајту Института, изузев одредаба чл. 12. који се примењују од 01.01.2021. године.

Измене и допуне овог Правилника врше се на исти начин и по поступку по коме је и донет.

В.Д. ДИРЕКТОРА ИНСТИТУТА „ВИНЧА"

проф. др Снежана Пајовић

Објављено на огласној табли и Web сајту Института за нуклеарне науке „Винча" дана 09.07.2020. године

Потврђује: