РЕПУБЛИКА СРБИЈА
ОСНОВНИ СУД У НИШУ
Су VIII 182/20
Дана 25.03.2021. године
Н И Ш

На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16, 94/17 и 77/19), члана 2. Уредбе о ближем садржају правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Сл. Гласник РС", бр. 94/2016), председник Основног суда у Нишу доноси:

ПРАВИЛНИК
о безбедности информационо - комуникационог система Основног суда у Нишу

I. Уводне одредбе

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности („Службени гласник РС", број 6/16, 94/17 и 77/19) и Уредбом о ближем садржају правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Сл. Гласник РС", бр. 94/2016), утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система Основног суда у Нишу (у даљем тексту: ИКТ систем).

Члан 2.

Примена мера заштите ИКТ система, које су прописане овим правилником, обавезујућа је за све запослене Основног суда у Нишу.

Непоштовање одредби овог правилника као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

За праћење примене овог правилника надлежан је председник суда и секретар суда.

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

1) *информационо комуникациони систем* (ИКТ систем) је технолошко организациона целина која обухвата све уређаје за електронску обраду података (хардверске и софтверске компоненте, мрежу и мрежне ресурсе, сервер и осталу комуникациону опрему);
2) *оператор ИКТ система* је Основни суд у Нишу као орган јавне власти, тј. државни орган;
3) *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;
4) *тајност* је својство које значи да податак није доступан неовлашћеним лицима;
5) *интегритет* значи очуваност изворног садржаја и комплетности податка;
6) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
7) *аутентичност* је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
8) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
9) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
10) *управљање ризиком* је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
11) *инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
12) *мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
13) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
14) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
15) VPN (Virtual Private Network)-је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
16) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
17) Backup је резервна копија података;
18) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
19) 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;
20) USB или флеш меморија је спољашњи медијум за складиштење података;
21) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;

22) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

II. Мере заштите

Члан 4.

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

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

Члан 5.

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 надлежан је систем администратор Основног суда у Нишу.

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност;
- послови управљање 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 Основног суда у Нишу, 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. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Рад на даљину и употреба мобилних уређаја у ИКТ систему није омогућен.

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 рукују запослени у складу са важећом систематизацијом радних места.

Систем администратор Основног суда у Нишу је дужан да сваког запосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Основног суда у Нишу.

Свако коришћење ИКТ ресурса Основног суда у Нишу 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 9.

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

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

О престанку радног односа или радног ангажовања, као и промени радног места, систем администратор је дужан да се информише у персоналној служби суда ради укидања, односно измене приступних привилегија за тог запосленог-корисника.

Корисник ИКТ ресурса, након престанка радног ангажовања у суду, 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 10.

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

Евиденцију о информационим добрима води систем администратор Основног суда у Нишу, 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 11.

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 12.

Подаци могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа поред систем администратора имати само запослени-корисници којима је то право омогућено.

Подаци (посебно они са ознаком тајности) могу да се сниме и на друге, преносне носаче података (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника.

Преносни носачи информација (медијуми) морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медијума са подацима, председник суда ће одредити одговорну особу и начин транспорта.

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

8. Ограничење приступа подацима и средствима за обраду података

Члан 13.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени има у складу са описом послова из важећег акта о систематизацији радних места.

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

Запослени је дужан 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 Основног суда у Нишу 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;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (backup) података у складу са прописаним процедурама;
13) користи интернет и електронску пошту у Основном суду у Нишу 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 14.

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 искључиво запослени у оквиру ИКТ службе.

Кориснички налог се састоји од јединственог 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 запосленог.

Кориснички налог додељује администратор на основу захтева судске управе а у складу са потребама обављања пословних задатака од стране запосленог.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева надлежног руководиоца.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Кориснички налог за приступ ИКТ систему Основног суда у Нишу се састоји од јединственог корисничког имена и лозинке.

Корисничко име се креира по матрици име.презиме, латиничним писмом без употребе слова ђ,ж,љ, њ, ћ, ч, џ, и ш.

Уместо ћириличних слова наведених у претходном ставу користе се латиничне ознаке за иста, и то: Ђ- DJ; Ж- Z, Љ-LJ, Њ-NJ, Ћ-C, Ч-C, Џ-DZ, Ш-S.

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 запосленог.

Ако запослени посумња да је друго лице открило његову лозинку дужан је да исту одмах измени и о томе обавести судску управу.

Запослени је дужан да мења лозинку најмање једном у два месеца.

Иста лозинка се не сме понављати у временском периоду од шест месеци.

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

Члан 16.

Приступ ресурсима ИКТ Основног суда у Нишу не захтева посебну криптозаштиту.

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.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује са као административна зона.

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

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

Члан 18.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система/запосленима на пословима ИКТ и осталим запосленима по овлашћењу председника суда.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система уз присуство администратора система.

Приступ административној зони може имати и запослени/а на пословима одржавања хигијене уз присуство администратора система.

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 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.

У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење председника суда који ће одредити услове, начин и место изношења опреме.

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

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

Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Основног суда у Нишу.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

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 председнику суда 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.

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

Члан 20.

ИКТ систем Основног суда у Нишу представља део јединственог информационог система правосудних органа. У складу са тим, превентивне мере као и мере заштите података прописане на нивоу ИКТ система правосудних органа примењују се и у ИКТ систему Основног суда у Нишу.

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

За успешну заштиту од злонамерног софтвера на сваком рачунару је инсталиран антивирусни програм при чему се свакодневно (аутоматски) врши допуна антивирусних дефиниција. Администратор система врши редовну контролу функционисања и ажурирања антивирусног програма.

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

Употреба преносних медија - USB меморија од стране корисника је омогућена. Пренос података са наведене врсте медија на рачунар у оквиру ИКТ система могућ је коришћењем USB меморија као и уз помоћ запослених на пословима ИКТ.

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 са интернета, у оквиру правосудне мреже запосленима је омогућен ограничени приступ интернету изузев запосленима на пословима ИКТ.

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

Запосленима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема) као и недозвољена употреба интернета која обухвата:

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

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

У циљу одговорног и сигурнијег коришћења сервиса електронске поште, неопходно је да се корисници придржавају одређених правила, и то:

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

пријаве на сервисе електронског банкарства, комуналних услуга и за друге приватне потребе);

- не приступати интернет линковима и отварању прилога (attachment-а) у склопу електронске поште који стижу са непознатих и сумњивих адреса пошиљалаца;
- не попуњавати (не слати) податке као што су на пр. корисничко име, лозинка, бр. телефона, алтернативна адреса електронске поште и сл. јер је у питању покушај злоупотребе;
- не прихватати опције за покретање неког програма/апликације уколико се при отварању документа из прилога појави порука типа „ок/сагласан";
- уколико нисте сигурни да ли је прилог (attachment) у поруци заражен или исправан дату поруку са прилогом (без отварања!!!) проследите вашим ИТ администраторима на проверу.

16. Заштита од губитка података

Члан 21.

Креирање резервних копија база података и медија фајлова врши се помоћу активних процедура једном дневно након радног времена. Копије се потом аутоматски пребацују (архивирају) на backup сервер.

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

Члан 22.

О активностима администратора и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др) и периодично (месечно, до 3. у месецу за претходни месец) достављају председнику суда.

Систем за контролу и дојаву о грешкама, неовлашћеним активностима и др, мора бити подешен тако да одмах обавештава администратора система, о свим нерегуларним активностима запослених-корисника, покушајима упада и упадима у систем и о томе одмах обавестите председника суда или секретара суда.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само запослени на пословима ИКТ.

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 24.

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

Подешавањем корисничких полиса од стране администратора система, онемогућено је неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

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

Члан 25.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених. Уколико то није могуће у радно време, онда се ревизија врши након завршетка радног времена уз претходну сагласност председника суда.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 26.

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 закључаним rack орманима, обезбеђена и лоцирана на прописаним местима и доступна систем администратору који је дужан да врши контролу целокупне 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 27.

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

Правила коришћења електронске поште, интернета и информационих ресурса прописана су на нивоу ИКТ система правосудних органа и чланом 20 овог Правилника.

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

Члан 28.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система спада у делокруг послова администратора система док су исти послови од стране трећих лица дефинисани уговором који је склопљен са тим лицима.

Председник суда контролише реализацију уговорених обавеза из претходног става или за то може овластити неко друго лице, уз претходно прибављено стручно мишљење од стране систем администратора.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система администратор система води документацију која садржи описе свих урађених процедура а посебно процедура које се односе на безбедност ИКТ система.

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

Члан 29.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести администратора система.

По пријему оправдане пријаве систем администратор је дужан да о томе обавести председника суда и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, „Сл. Гласник РС", бр, 11/2020), систем администратор је дужан да поред председника суда обавести и надлежни орган дефинисан овом уредбом.

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.

25. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 30.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде суда, запослени на пословима ИКТ, је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује 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 председника суда.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди председник суда. Складиштење делова ИКТ система који нису неопходни, се врши тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води.

III. Измена Правилника о безбедности

Члан 31.

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 председника суда, како би он могао да приступи измени овог правилника, у циљу унапређења 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 32.

Проверу ИКТ система врши систем администратор Основног суда у Нишу.

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 председнику суда.

V. Садржај извештаја о провери ИКТ система

Члан 33.

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава;
2) време провере;
3) подаци о лицима која су вршила проверу;
4) извештај о спроведеним радњама провере;
5) закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;
6) закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
7) закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система;
8) оцена укупног нивоа информационе безбедности;
9) предлог евентуалних корективних мера;
10) потпис одговорног лица које је спровело проверу ИКТ система.

VI. Прелазне и завршне одредбе

Члан 34.

Овај правилник ступа на снагу даном објављивања на огласној табли и интернет страници Основног суда у Нишу.

У Нишу, дана 25.03.2021.

Председник Основног суда у Нишу