06.03.24

Република Србија
ОСНОВНИ СУД У СЈЕНИЦИ
Су бр. I-1-2/2024
Дана 01.03.2024. године,
СЈЕНИЦА

На основу члана 8. Закона о информционој безбедности („Службени гласник РС“ број 6/2016 и 94/2017), члана 2. Уредбе о ближем садржају правилника о безбедности информационо комуникационих система од посебног значаја, начину провере информационо комуникационих система од посебног значаја („Службени гласник РС“ број 94/2016) и члана 59. Закона о агенцији за борбу против корупције („Службени гласник РС“, број 97/2008, 53/2010, 66/2011, 67/2013, 8/2015), председник суда доноси:

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО КОМУНИКАЦИОНОГ СИСТЕМА ОСНОВНОГ СУДА У СЈЕНИЦИ

УВОДНЕ ОДРЕДБЕ
Члан 1.

Овим Правилником уређују се мере заштите информационо-комуникационог система у Основном суду у Сјеници, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса у суду.

Члан 2.

Циљеви доношења овог Акта су:

- допринос постизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
- минимизација безбедносних инцидената;
- допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистентне контроле свих компонената информационо-комуникационог система (у даљем тексту ИКТ систем).

Члан 3.

Овај акт је обавезујући за све кориснике информатичких ресурса, ка и за сва трећа лица која користе информатичке ресурсе суда.

Непоштовање овог Акта повлачи дисциплинску одговорност корисника информатичких ресурса.

За праћење примене овог Акта надлежан је председник суда, као и судска управа.

Члан 4.

Поједини појмови у смислу овог правилника имају следеће значење:

1. информационо-комуникациони систем (ИКТ систем) је технолошка организациона целина која обухвата:
   1.1. електронске комуникационе мреже у смислу закона који уређују 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 у сврху њиховог рада, употребе, заштите или одржавања;
   1.4. 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 неовлашћених лицима;
4. интегритет значи очуваност изворног садржаја и комплетности података;
5. расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
6. аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
7. непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
8. ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
9. управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима.
10. инцидент је унутрашња или спољашња 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. информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и сл.;
13. VPN (Virtual Private Network) – је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
14. Администратор ИКТ система – лице које има администраторски налог који омогућава који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога.
15. BACKUP је резервна копија података;
16. ЦИТ – Центар за информационе технологије чији је задатак управљање ИКТ сходно Акту о систематизацији радних места и послова.

МЕРЕ ЗАШТИТЕ
Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидента који угрожавају обављање делатности суда, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Мере заштите ИКТ система обухватају следеће послове:

1. Успостављање организационе структуре са утврђеним пословима и одговорностима запослених, који су оспособљени за посао који раде и разумеју своју одговорност;

2. Ограничење приступа подацима и средствима за обраду података (рачунарима);

3. Онемогућавање, односно спречавање неовлашћене или ненамерне измене, губитка, оштећења или злоупотребе података и средстава уа обраду података;

4. Заштита података и средстава за обраду података од злонамерног софтвера;

5. Обезбеђивање исправног и безбедног функционисања средстава за обраду података;

6. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код Оператора ИКТ система;

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

8. Превенција и реаговање на безбедносне инциденте, пријављивање недостатака и предлагање одговарајућих мера у циљу побољшања информационе безбедности.

АДМИНИСТРАТОР ИКТ СИСТЕМА

Члан 6.

ИКТ системом управља и руководи запослени који поседује администраторски налог, у складу са описом послова из важећег акта о систематизацији радних места.

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

Запослено лице које 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.

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

Запослени који управља ИКТ системом (администратор) дужан је да сваког новог корисника упозна са одговорностима и правилима коришћења ИКТ ресурса суда и да води евиденцију о изјавама новозапослених корисника да су упознати са правилима коришћења ИКТ ресурса.

Евиденцију о информационим добрима суда води администратор ИКТ система у папирној или електронској форми.

НАЛОЗИ КОРИСНИКА

Члан 7.

Кориснички налог се састоји од корисничког имена и лозинке.

Кориснички налог се креира на тај начин сто се прво уписује име, па презиме запосленог, која су одвојена тачком и куцају се латиницним писмом без употребе слова Ђ; Ж; Љ; Њ; Ћ; Ч; Џ; Ш.

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

Лозинка корисника 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 корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Корисник је дужан да мења лозинку на свака два месеца.

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

Члан 8.

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

Кориснички налог додељује администратор у сарањи са непосредним руководиоцем.

За послове извршене под одређеним корисничким именом и лозинком одговоран је корисник ИКТ система које је корисничко име, тј. налог додељен.

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

ОГРАНИЧЕЊЕ ПРИСТУПА ПОДАЦИМА И СРЕДСТВИМА ЗА ОБРАДУ ПОДАТАКА

Члан 9.

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

Запослени који има администраторски налог, има право 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 злоупотребљава 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 суда;
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 инсталацијусофтвера или хардвера подноси у писаној форми, одобрен од стране руководиоца или судије;
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 д анеовлашћено инсталира други антивирусни програм;
11. На радној станици не сме да складишти садржај који не служи у пословне сврхе;
12. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
13. Прихвати да технике сигурности (анти-вирусни програми, заштитни сид (firewall) системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему.
14. Не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

НАДЗОР И КОНТРОЛА ОД СТРАНЕ АДМИНИСТРАТОРА

Члан 10.

Администратор ИКТ система у обавези је да континуирано надзире и проверава функционисање средстава за обраду података, да управља ризицима који могу утицати на безбедности ИКТ система, као и да планира и предлаже руководиоцу одређене мере.

Администратор ИКТ система је дужан да проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, да врши проверу безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система, архитектуре решења, техничке конфигурације.

О извршеној провери сачињава извештај и доставља руководиоцу. Извештај треба да садржи време провере, спроведене радње, закључке по питању адекватне примене предвиђених мера заштите, закључке по питању евентуалних безбедносних слабости, оцену стања у погледу информационе безбедности, предлог евентуалних корективних мера и потпис лица које је спровело проверу ИКТ система.

ПРЕСТАНАК РАДНОГ ОДНОСА ЗАПОСЛЕНОГ И ПРОМЕНА РАДНОГ МЕСТА И ОВЛАШЋЕЊА

Члан 11.

У случају промене радног места, односно овлашћења корисника, администратор ИКТ система ће извршити промену права у коришћењу ИКТ система, у складу са описом радних задатака и захтевом руководиоца корисника система.

У случају престанка радног ангажовања корисника, његов кориснички налог се гаси тј. укида.

О престанку радног односа или радног ангажовања, као и промени радног места корисника, руководилац је дужан да обавести администратора ИКТ система, ради укидања, односно измене приступних налога тог корисника.

Корисник је након престанка правног основа по коме је приступао ресурсима ИКТ система суда, у обавези да не открива податке који су од значаја за информациону безбедност ИКТ система.

ПРЕНОСИВИ МЕДИЈИ И АНТИВИРУСНА ЗАШТИТА

Члан 12.

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 меморијом, CD-ом, итд), инсталацијом нелиценцираног софтвера и слично.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм.

Свакодневно се аутоматски у тачно одређено време врши допуна антивирусних дефиниција.

Забрањено је заустављање или искључивање антивирусног софтвера.

Преносиви медији (USB меморија, CD) пре коришћења морају бити проверени на присуство вируса од стране администратора ИКТ система.

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

ПОСТУПАЊЕ СА ОПРЕМОМ ИКТ СИСТЕМА

Члан 13.

Простору у коме се налазе сервер, мрежна и комуникациона опрема има право приступа само администратор 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 и уз присуство надлежног лица.

Приступ административној зони може имати и запослени на пословима одржавања.

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.

У простору је неопходно успоставити и одржавати одговарајућу температуру, у складу са важећим стандардима (климатзован простор).

Прозори и врата на просторији из става 1. овог члана морају увек бити затворени.

Сервер и 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, администратор ИКТ система је дужан да искључи опрему у складу са процедурама произвођача опреме.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходно стабилну врзију.

Инсталирање новог софтвера, као и ажурирање постојечег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запосленог-корисника.

Члан 14.

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

Мрежна опрема (Switch, Router) се мор аналазити у закључаном Rack орману.

Администратор ИКТ система врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Члан 15.

У случају изношења опреме ИКТ система ради сервисирања, неопходно је писано одобрење руководиоца.

Администратор ИКТ система одређује све детаље везане за изношење опреме и сачињава записник у коме се наводи назив и тип опреме, серијски број, назив сервисера.

У случају крајње нужде, у циљу спашавања опреме, иста се може изнети без одобрења руководиоца.

РЕЗЕРВНЕ КОПИЈЕ ПОДАТАКА

Члан 16.

Администратор ИКТ система је у обавези да прави резервне копије база података најмање једном дневно.

Базе података обавезно се архивирају и на преносиве медије (CD Rom, DVD, USB, екстерни хард диск). За потребе обнове базе података 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 које је извршио копирање-архивирање.

Дневне, недељне и месечне копије-архиве се чувају у просторији која је физички обезбеђена у складу са мерама заштите од пожара, поплава и слично.

Исправност копије-архива проверава администратор ИКТ система.

ЗАВРШНЕ ОДРЕДБЕ

Члан 17.

Правилник ступа на правну снагу даном објављивања на огласној табли суда, где ће бити изложен 30 дана, како би се сви запослени упознали са истим.

Правилник објавити и на интернет страници суда.

ПРЕДСЕДНИК СУДА

Машовић Алмир