РЕПУБЛИКА СРБИЈА
ОСНОВНИ СУД
Су бр. I-1-97/21
09.09.2022.године
В Р А Њ Е

На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС", бр. 94/2016), као и на основу члана 52. Закона о уређењу судова („Сл. Гласник РС" бр. 116/08, 104/09, 101/10, 31/2011-др. Закон 78/2011-др.закон, 101/11, 101/13, 106/15, 40/15-др. Закон, 13/2016, 108/2016, 113/2017, 65/2018- одлука УС, 87/2018 и 88/2018-одлука УС), чланова 6.и 7. Судског пословника ("Службени гласник РС", бр. 110/2009, 70/2011, 19/2012, 89/2013, 96/2015, 104/2015, 113/2015 - испр, 39/2016, 56/2016, 77/2016, 16/2018, 78/2018, 43/2019 и 93/2019), председник Основног суда у Врању Драгана Станковић-Тасић, дана 09.09.2022. године, доноси

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ОСНОВНОГ СУДА У ВРАЊУ

I. Уводне одредбе

Члан 1.

Овим правилником ближе се утврђују мере заштите информационо-комуникационог система (у даљем тексту ИКТ систем), принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења, дужности и одговорности корисника информатичких ресурса у Основног суда у Врању.

Члан 2.

Циљеви доношења правилника о безбедности су:

- унапређење информационе безбедности и контроле свих компоненти ИКТ система;

- подизање свести запослених о ризицима и мерама заштите приликом коришћења информационих технологија;
- минимизација безбедоносних ризика.

Члан 3.

Мере се односе на све организационе јединице Основног суда у Врању, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе суда.

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса.

За праћење примене овог Акта надлежан је систем администратор Основног суда у Врању-

Члан 4.

Поједини термини у смислу овог правилника имају следеће значење:

1) ИКТ систем је технолошко-организациона целина која обухвата:
а) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
б) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
в) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачке (а) и (б) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
г) организациону структуру путем које се управља ИКТ системом;

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

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

4) интегритет значи очуваност изворног садржаја и комплетности податка;

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

6) аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

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

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

9) управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

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

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

12) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

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

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

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

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

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

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

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

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

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

22) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;

23) Backup је резервна копија података;

24) Download је трансфер података са централног рачунара или web презентације на локални рачунар;

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

26) Freeware је бесплатан софтвер;

27) Opensource софтвер отвореног кода;

28) Firewall је „заштитни зид" 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 спољњи медијум за складиштење података;

30) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;

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

II. Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожава обављање делатности суда, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, коришћења, промене или брисања података, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

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

Члан 6.

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

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система Основног суда у Врању падлежан је систем администратор Основног суда у Врању.

Члан 7.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност;
- послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности;
- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Основног суда у Врању, 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.

У случају настанка инцидента, корисник информатичких ресурса дужан је да у циљу решавања, пријави инцидент непосредном руководиоцу или систем администратору.

Руководилац службе за информатику и аналитику у зависности од значаја и врсте инцидента, обавештава управу суда.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 8.

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 9.

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места.

Непосредни руководиоци су дужни да сваког новозапосленог корисника ИКТ система упознају са одговорностима и правилима коришћења ИКТ ресурса суда.

Свако коришћење ИКТ ресурса Основног суда од стране запосленог-корисника, ван додељених овлашћење, подлеже дисциплинској одговорности.

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

Члан 10.

У случају промене послова, односно надлежности корисника-запосленог, непосредни руководилац је дужан да обавестити систем администратора Основног суда у Врању који ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака које запослени обавља.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида на основу захтева непосредног руководиоца.

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

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра Основног суда у Врању су сви ресурси који садрже пословне информације суда у електронском облику или служе за приступ корисника ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију и слично, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему.

Евиденцију о информационим добрима води систем администратор Основног суда у Врању.

Предмет заштите су:
- хардверске и софтверске компоненте ИКТ система;
- подаци који се обрађују или чувају на компонентама ИКТ система;
- кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система.

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

Члан 12.

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

7. Заштита носача података

Члан 13.

Служба за информатику и аналитику ће успоставити организацију приступа и рада са подацима, посебно онима који су од стране судске управе означени степеном

службености или тајности у складу са Законом о тајности података (Службени гласник РС бр.104/09):

- подаци и документи са ознаком тајности снимају се на засебном серверу-рачунару или у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено.

- подаци и документи као и подаци са ознаком тајности могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника.

Евиденцију носача података означених степеном тајности воде овлашћена лица у писарници или судској управи. Остале евиденције носача података води служба за информатику и аналитику. Сви медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, председник суда 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.

8. Ограничење приступа подацима и средствима за обраду података

Члан 14.

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

Запослени који имају администраторски налог, имају права приступа свим ресурсима ИКТ система (софтверским, хардверским и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Запослени-корисник може користити само свој кориснички налог који је добио од администратора.

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

Запослени-корисник дужан је да поштује и следећа правила ради безбедног и примереног коришћења ресурса ИКТ система:

- користи информатичке ресурсе искључиво у пословне сврхе;
- прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Основног суда у Врању и да могу бити предмет надгледања и прегледања;
- поступа са поверљивим подацима у складу са прописима и води рачуна о сигурности података;
- безбедно чува своје лозинке, мења их периодично, не одаје их другим лицима;
- пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу

- приступа информатичким ресурсима само на основу додељених корисничких права;

- не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;

- на радној станици не сме да складишти садржај који не служи у пословне сврхе;

- израђује заштитне копије (backup) података у складу са прописаним процедурама;

- користи електронску пошту у суду у складу са прописаним процедурама;

- 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;

- не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 15.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља.

Корисници могу да имају администраторски или кориснички налог који се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу чега се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

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 може да користи само систем администратор и лице које га у случају спречености замењује.

Кориснички налог додељује администратор након евиденције запосленог у јединици за кадровске послове, а на основу захтева непосредног руководиоца и у складу са потребама обављања пословних задатака од стране запосленог-корисника.

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

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 16.

Аутентификација корисника којима је одобрен приступ систему врши се путем јединственог корисничког налога који се састоји од имена и лозинке.

Корисничко име се креира латиничним писмом по матрици име.презиме.

Уколико два корисника имају исто име и презиме, између се додаје средње слово или више, одвојено тачкама.

Уколико два корисника имају исто име и презиме, додаје се и друго или треће слово имена.

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

Запослени-корисник дужан је да мења лозинку најмање једном у годину дана или чешће кад то систем захтева од њега, након истека системски подешеног периода за промену лозинке.

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

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

Члан 17.

Приступ ресурсима ИКТ система Основног суда у Врању не захтева посебну криптозаштиту.

Запослени-корисници које судска управа или непосредни руководилац одреди, користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама и порталима ван суда, сходно радним задацима које обављају.

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

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

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

Члан 18.

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

Простор треба 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 19.

Улаз у просторију (сервер салу) у којој се налази ИКТ опрема, дозвољен је само систем администратору.

Осим систем администратора, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу судске управе или надлежног руководиоца, и уз присуство систем администратора или лица које га замењује.

Просторија мора бити 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 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 сл.) може изнети и без одобрења судске управе.

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

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 20.

Систем администратор проверава функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и у складу са тим, руководилац службе планира и предлаже судској управи/председнику суда 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.

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

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

Члан 21.

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

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

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

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

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

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави служби за информатику и аналитику.

Судска управа одређују ниво приступа интернету сходно потребама посла.

Корисници ИКТ система који користе интернет на рачунарима локалне судске мреже, морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени-корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши систем администратор и ИКТ служба Министарства правде.

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

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

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема).

16. Заштита од губитка података

Члан 22.

Израда резевних копија базе података се обавезно врши на серверу суда или на преносиве медије (CD, DVD, екстерни хард диск, сториџ систем), једном дневно за потребе обнове базе података.

Израда резервних копија идентификованих фолдера, фајлова-докумената се врши једном месечно.

Израда дневних резервних копија података се врши сваки радни дан у недељи.

Израда месечних резервних копија података се врши последњег радног дана у месецу.

Сваки примерак преносног информатичког медија са копијама-архивама је означен бројем, врстом садржаја и датумом израде копије-архиве.

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.

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

Члан 23.

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

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Министарства правде или Основног суда у Врању, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера могу да врше запослени у служби за информатику и аналитику.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера, уз присуство најмање једног запосленог из Основног суда у Врању.

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

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

Систем администратор подешава корисничке полисе у циљу спречавања неовлашћеног инсталирање софтвера који може довести до угрожавања безбедности ИКТ система и по потреби прати и анализира дневник активности у циљу идентификације потенцијалних слабости ИКТ система.

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

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

Члан 26.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених.

Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност председника суда.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 27.

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

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

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

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

Члан 28.

Размена података са државним органима, правним и физичким лицима се врши у складу са важећим прописима и унапред дефинисаними потписаним уговорима.

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

Члан 29.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Основног суда у Врању, дефинише се уговором склопљеним са тим лицима.

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

Документација, упутства и процедуре добијена од трећих лица при инсталацији или замени ресурса ИКТ система чувају се у просторијама службе.

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

Члан 30.

За потребе тестирања ИКТ система, односно делова система могу се користити само оперативни подаци који нису осетљиви.

Приликом тестирања система не могу се користити подаци који представљају податке о личности, нити подаци који су под ознаком тајности, односно службености као поверљиви подаци.

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

Члан 31.

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само софтверу који су они израдили и подацима који нису осетљиви, односно за које постоји уговором дефинисан приступ уз контролу.

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

Члан 32.

Служба за ИКТ Основног суда у Врању – систем администратор је одговоран 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 систем администратор је дужан да одмах обавести судску управу.

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

Члан 33.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести непосредног руководиоца или систем администратора Основног суда у Врању.

По пријему пријаве систем администратор је дужан да одмах предузме мере у циљу заштите ресурса ИКТ система.

У зависности од врсте и значаја инцидента систем администратор обавештава судску управу.

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

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 34.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Основног суда у Врању систем администратор је дужан да по налогу судске управе у најкраћем року пренесе делове ИКТ 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 Основног суда у Врању, 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 у судској управи.

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. ИзменаПравилника о безбедности

Члан 35.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, руководилац Службе за информатику и аналитику је дужан да обавести судску управу, како би се приступило измени овог правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IV. Провера ИКТ система

Члан 36.

На захтев судске управе врши се провера ИКТ система.

Проверу ИКТ система систем администратор.

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;

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 судској управи.

V. Садржај извештаја о провери ИКТ система

Члан 37.

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава;
2) време провере;
3) подаци о лицима која су вршила проверу;
4) извештај о спроведеним радњама провере;
5) закључке по питању усклађености 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 38.

Правилник о безбедности информационог комуникационог система објавити на интернет страници суда.

ПРЕДСЕДНИК СУДА,
Драгана Станковић-Тасић