Република Србија
ПРЕКРШАЈНИ СУД У ПОЖЕГИ
Су бр. I – 526 /17
Дана, 08.06.2017.године
П о ж е г а

На основу члана 8. Закона о информационој безбедности ("Службени гласник РС", број 6/16), чланова 1-8 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 од 24.11.2016. године), Председник Прекршајног суда у Пожеги доноси:

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО – КОМУНИКАЦИОНИХ СИСТЕМА ПРЕКРШАЈНОГ СУДА У ПОЖЕГИ

I.Уводне одредбе

Члан 1

Овим правилником ближе се дефинишу мере заштите информационо-комуникационих система у Прекршајном суду у Пожеги, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информационо-комуникационих система (у даљем тексту ИКТ систем).

Члан 2

Циљеви доношења овог Правилника су:

- допринос подизању 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 ИКТ система.

Члан 3

Овај Правилник је обавезујући за све унутрашње организационе јединице Прекршајног суда у Пожеги и за све кориснике информатичких ресурса, као и за сва трећа лица која користе информатичке ресурсе Прекршајног суда.
Непоштовање овог Правилника повлачи дисциплинску одговорност корисника информатичких ресурса.
За праћење примене овог Правилника 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 технолошко-организациона целина која обухвата:
    - електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
    - уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно да се у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
    - податке који се потхрањују, обрађују, претражују или преносе у сврху њиховог рада, употребе, заштите или одржавања;
    - 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 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 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 одговарајућим степеном тајности;
13. Криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
14. информациона добра обухватају податке у датотекама и базама података, програмски код, 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. WAN (Wide Area Network) је мрежа широког подручја која покрива веће земљописно подручје(градове, државе или континенте) и обично се користи за међусобно повезивање удаљених рачунара или локалних (LAN) мрежа.
17. Администратор ИКТ система - лице које има администраторски налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога.
18. Backup је резервна копија података;
19. Download је трансфер података са централног рачунара или web презентације на локални рачунар;
20. MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
21. UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
22. Freeware је бесплатан софтвер;
23. Opensource софтвер отвореног кода;
24. 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;
25. USB или флеш меморија је спољни медијум за складиштење података;
26. CD-ROM (Compact disk – read only memory) користи се као медијум за складиштење података;
27. DVD је оптички диск високог капацитета који се користи за складиштење података.

II. Мере заштите

Члан 5

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

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којима се остварује управљање информационом безбедношћу у Прекршајном суду у Пожеги

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 надлежан је систем администратор Прекршајног суда у Пожеги.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су подешени од стране систем администратора, да приступају само одређеним деловима ИКТ система. Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ.

Запосленом-кориснику забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима.

Систем администратор свакодневно контролише приступ ресурсима ИКТ система и проверава има ли приступа са непознатих уређаја (са непознатих MAC адреса) и ако се установи неовлашћен приступ та MAC адреса се уноси у „block“ листу софтвера који се користи за контролу приступа.

У случају квара мобилног уређаја, систем администратор је дужан да пре предаје уређаја овлашћеном сервису, уради копију података који се налазе на мобилном уређају, а потом их обрише из уређаја, и по повратку из сервиса поново врати податке у мобилни уређај.

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

Члан 8

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места. Систем администратор је дужан да сваког корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Прекршајног суда у Пожеги.

Свако коришћење ИКТ ресурса Прекршајног суда у Пожеги 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 запосленог-корисника ИКТ система

Члан 9

У случају промене послова, односно надлежности корисника-запосленог, администратор система 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.

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 су сви ресурси који садрже пословне информације Прекршајног суда у Пожеги, 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 у папирној или електронској форми.

Предмет заштите обухвата:

1. хардверске и софтверске компоненте информатичких ресурса
2. податке који се обрађују или чувају на информатичким ресурсима
3. корисничке налоге и друге податке о корисницима информатичких ресурса у Прекршајном суду

6. Класификовање података тако да ниво 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 имати само запослени-корисници којима је то право обезбеђено одлуком Председника суда.

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

Носачи информација морају бити прописано обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта носача информација Председник суда ће одредити одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на носачима, подаци морају бити трајно обрисани, ако то није могуће, такви носачи 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-корисник има.

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

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

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

Запослени-корисник дужан је да поштује и следећа правила безбедног и примерног 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 Прекршајног суда у Пожеги;
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 података у складу са прописаним процедурама;
13. користи интернет и електронску пошту у складу са прописаним процедурама;
14. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
15. 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.
16. 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 може да користи искључиво систем администратор Прекршајног суда.

Кориснички налог се састоји од 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-корисника.

Кориснички налог додељује администратор, на основу захтева запосленог задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

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

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира латиничним писмом по матрици (прво слово имена и цело презиме) као једна реч раздвојено једино тачком и без употребе слова ђ, ж, љ, њ, ћ, ч, џ, ш.

Лозинка мора да садржи минимум осам карактера, састављених комбинацијом латиничних великих и малих слова као и бројева. Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке.

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

Запослени-корисник дужан је да мења лозинку једном месечно и иста лозинка не сме да се понавља у временском периоду од годину дана.

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

Део пријављивања у ИКТ систем Прекршајног суда у Пожеги врши се убацивањем медија са електронским сертификатом у читач картице.

Неовлашћено уступање корисничког налога као и медија са електронским сертификатом другом лицу, подлеже дисциплинској одговорности.

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

Члан 16

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови:

1. сервери, сторици и комуникационо чвориште у просторијама суда морају бити смештени у посебној просторији (сервер соби), која испуњава стандарде противпожарне заштите и поседује непрекидно напајање електричном енергијом и адекватну климатизацију и којој је забрањен приступ незапосленим лицима;
2. приступ сервер соби, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење Председника суда;

3. радна станица мора да буде примерно физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компоната;
4. просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;
5. штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;
6. медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

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

Члан 17

Улаз у просторије у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система и запосленим-корисницима ИКТсистема.
Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу Председника суда и уз присуство надлежног лица.
Приступ административној зони могу имати и лица која пружају услуге одржавања хигијене уз присуство надлежног лица.
Административна зона мора имати противпожарну опрему која се користи 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 електричном енергијом - UPS.
У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а овлашћено лице дужно је да искључи опрему у складу са процедурама произвођача опреме.
ИКТ опрема се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења Председника суда.
У случају изношења опреме ради селидбе или сервисирања, неопходно је одобрење Председника суда који ће одредити услове, начин и место изношења опреме.
Ако се опрема износи ради сервисирања, поред одобрења Председника суда систем администратор је дужан да сачини записник у коме се наводи назив и тип опреме, серијски број, назив сервисера и кратак опис квара.
Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Прекршајног суда у Пожеги.

13. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 18

Запослени на пословима ИКТ система 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 архиве 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 сучају 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.

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

Члан 19

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 меморије, CD итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од злонамерног софтвера Прекршајни суд у Пожеги своју делатност обавља преко „Правосудне“ WAN мреже која има ограничен приступ, такође на сваком рачунару је инсталиран антивирусни програм који се свакодневно аутоматски ажурира.

У циљу заштите од ИКТ система од малициозног софтвера неопходна је примена лиценцираног софтвера, односно забрана неауторизованог софтвера.

Преносиви медији пре коришћења морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, врши се чишћење медија од вируса, уз сагласност доносиоца медија. Ризик од евентуалног губитка података приликом чишћења медија антивирусним софтвером, сноси доносилац медија.

Запосленим-корисницима који су прикључени на ИКТ систем, строго 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 оговарајући 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;
- преузимања (download) података велике „тежине“ који проузрокују „загушење“ на мрежи;
- преузимање (download) материјала заштићених ауторским правима;

- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостриминг и сл.);
- недозвољен приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета

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

У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

- електронска пошта са прилозима не сме се отварати ако долази са сумљивих и непознатих адреса, већ се мора избрисати;
- забрањено је коришћење електронске поште у приватне сврхе (не смеју се користити пословни налози електронске поште у приватне сврхе)

15. Заштита од губитка података

Члан 20

Заштита од губитка података у Прекршајном суду у Пожеги обезбеђује се креирањем резервних копија на екстерном диску који је прописано обележен и чува се на обезбеђеном месту. Свака радна станица има конфигурисан секундарни хард диск на коме се копирају подаци. Сви документи штампани из ИКТ система се меморишу као ПДФ документи.

16. Обезбеђење интегритета софтвера и оперативних система

Члан 21

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца, односно Freewere i Opensource верзије.

Инасталацију и подешавање софтвера може да врши само систем администратор Прекршајног суда у Пожеги.

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.

17. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 22

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.

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

18. Обезбеђење да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Члан 23

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.

19. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 24

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) мора бити обезбеђена и лоцирана на прописаним местима, доступна систем администратору које је дужан да врши контролу целокупне мрежне опреме и благовремено преузима мере у циљу отклањања евентуалних неправилности.

Безжична мрежа коју могу користити посетиоци објекта у надлежности Прекршајног суда у Пожеги мора бити одвојена од интерне мреже коју користе запослени-корисници суда, кроз коју се врши размена службених података.

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

Члан 25

Преносиви медији који садрже податке морају да буду прописано обележени и пописани.

Пренос медија као и начин преноса унутар и ван оператора ИКТ система одређује Председник суда.

Преносиви медији пре стављања ван употребе морају бити физички уништени.

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

Члан 26

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система спада у делокруг послова систем администратора, док су исти послови са трећим лицима дефинисани уговором склопљеним са тим лицима.

Председник суда је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица или за ту врсту посла може овласти друго лице (систем администратора).

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система, администратор система мора да води документацију која садржи описе свих урађених процедура.

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

Члан 27

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

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

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

23. Мере које обезбеђују континуитет обављања посла у ванредним ситуацијама

Члан 28

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде суда систем администратор 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 је један код њега, други код надлежног органа за послове одбране и ванредне ситуације, а трећи примерак код Председника суда.

Делови ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди Председник суда.

III. Измена Правилника о безбедности

Члан 29

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 ресурса ИКТ система.

IV. Провера ИКТ система

Члан 30

Проверу ИКТ система врши систем администратор Прекршајног суда у Пожеги.

V. Садржај извештаја о провери ИКТ система

Члан 31

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;
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 адекватне примене предвиђених мера заштите у оперативном раду;
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 32

Овај Правилник ступа на снагу наредног дана од дана објављивања на огласној табли и интернет страници Прекршајног суда у Пожеги.

Пожега, 08.06.2017. године

ПРЕДСЕДНИК ПРЕКРШАЈНОГ СУДА

Горица Весовић