Република Србија
Виши суд у Крагујевцу
СУ-I-1-27/23
28.03.2023. године
К р а г у ј е в а ц

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС", број 6/16, 94/17 и 77/19), чл. 2. и 3. 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), председник Вишег суда у Крагујевцу, Весна Миловановић доноси

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ВИШЕГ СУДА У КРАГУЈЕВЦУ

I ОСНОВНЕ ОДРЕДБЕ
Предмет правилника

Члан 1.

Правилником о безбедности информационо-комуникационог система Вишег суда у Крагујевцу ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система Вишег суда у Крагујевцу (у даљем тексту: ИКТ систем).

Циљеви правилника

Члан 2.

Циљеви доношења правилника су:

-одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;

-спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;

-подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;

-прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;

-свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби правилника

Члан 3.

Запослени у Вишем суда у Крагујевцу морају бити упознати са садржином правилника и дужни су да поступају у складу са одредбама овог правилника, као и других интерних процедура које регулишу информациону безбедност.

Мере се односе на све запослене - кориснике информатичких ресурса у Вишем суду у Крагујевцу, као и на трећа лица која користе информатичке ресурсе суда.

Служба за информатичке послове и судска управа надлежни су за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим правилником и интерним процедурама

Одговорност запослених

Члан 4.

Запослени у Вишем суду у Крагујевцу су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

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

Поједини термини у смислу овог правилника имају следеће значење:

1. *информационо-комуникациони систем (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 воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. а) и б) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

г) организациону структуру путем које се управља ИКТ системом;

д) све типове системског и апликативног софтвера и софтверске развојне алате.

2. *оператор ИКТ система* је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

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 сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система;

11.а) *јединствени систем за пријем обавештења о инцидентима* је информациони систем у који се уносе подаци о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности;

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

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

16. *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о

коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично;
17. *Freeware* је бесплатан софтвер;

18. *Opensource* софтвер отвореног кода;

19. *USB или флеш меморија* је спољшњи медијум за складиштење података;

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

21. *DVD* је оптички диск високог капацитета који се користи као медијум за складиштење података;

22. *Backup* је резервна копија података.

Предмет 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.

II МЕРЕ ЗАШТИТЕ

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

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 Вишег суда у Крагујевцу надлежна је служба за информатичке послове. Виши суд у Крагујевцу смештен је у Палати правде са другим органима тако да се користе и заједничке просторије. Део послова везаних за област безбедности ИКТ система Вишег суда у Крагујевцу мора се ускладити и са другим органима, управе Вишег суда и Министарства правде које је надлежно за део послова из области безбедности а које су у вези са радом Вишег суда у Крагујевцу.

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 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 Вишег суда у Крагујевцу, 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, служби за информатичке послове или судској управи.

Руководилац службе за инфорамтичке послове у зависности од значаја и врсте инцидента, обавештава управу суда.

Одговорно лице (руководилац службе за информатичке послове - систем администратор) за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности, поступа у складу са одговарајућом процедуром.

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 управљају запослени у складу са важећом систематизацијом радних места. Службу за информатичке послове чине, руководилац службе за информатичке послове – систем администратор (образовање - дипломирани инжењер електротехнике, звање- саветник) и техничар за ИТ подршку (образовање - електротехничар рачунара, звање - референт).

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

Свако коришћење ИКТ ресурса Вишег 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 9.

У случају промене послова, односно надлежности корисника-запосленог, управа суда ће обавестити службу за информатичке послове Вишег суда у Крагујевцу која 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 обавештења управе суда.

Корисник ИКТ ресурса, након престанка радног ангажовања, 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 Вишег суда у Крагујевцу 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 служба за информатичке послове Вишег суда у Крагујевцу.

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 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.

Служба за информатичке послове 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 начин којим ће право приступа имати само запослени-корисници којима је то право обезбеђено.

Подаци и документа могу се снимати на серверу, у фолдерима где постоји одређена организација приступа и на локалним рачунарима. Подаци и документа могу бити снимљени (сачувани) од стране овлашћених запослених-корисника на другим носачима (екстерни хард диск, USB,CD, DVD) .

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 13.

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 Вишег суда у Крагујевцу 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 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 14.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Запосленом у складу са радним местом и пословима које обавља додељује се налог који се састоји од корисничког имена и шифре.

Корисници могу да имају администраторски или кориснички налог.

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 само запослени у служби за информатичке послове.

Кориснички налог додељује администратор на основу захтева судске праве 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 судске управе.

Поред налога за приступ ИКТ систему, корисник-запослени може имати налог који се састоји од корисничког имена и шифре за АВП, електронску пошту, апликације, портале и др.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15.

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

Запослени-корисник дужан је да мења лозинку периодично или кад то систем захтева од њега, након истека системски подешеног периода за промену лозинке.

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

Сви корисници су дужни да:

• корисничко име и шифру држе у тајности, не откривају их другим лицима
• промене шифру када примете да постоји било какав наговештај могућег компромитовања.

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

Члан 16.

Приступ ресурсима ИКТ система Вишег суда у Крагујевцу 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 17.

Простор у коме се налазе сервери Вишег суда у Крагујевцу је заједнички за органе смештене у Палати правде у Крагујевцу. Све активности везане за одржавање овог простора Служба за информатичке послове Вишет суда у Крагујевцу радиће по налозима и захтевима Министарства правде, управе Вишег суда у Крагујевцу и заједничке службе.

Улаз у просторију у којој се налази ИКТ опрема а која припада само Вишем суду у Крагујевцу, који је смештен у Палати правде, дозвољен је само запосленима у служби за информатичке послове Вишег суда у Крагујевцу и судској управи.

Просторија у којој је смештен део ИКТ опреме и осетљиви подаци који се чувају и користе у служби за информатичке послове има и контролисани систем улаза са идентификационим картицама. Право улазка са картицама имају запослени у служби за информатичке послове и у управи суда.

Приступ овим просторијама може имати и запослени на пословима одржавања хигијене уз присуство једног запосленог из службе за информатичке послове или судске управе.

Сви остали запослени, због потребе посла, у овим просторијама могу бити само уз присуство једног запосленог из службе за информатичке послове или управе суда.

Приступ овим просторијама могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу судске управе, и уз присуство једног запосленог из службе за информатичке послове.

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

Члан 18.

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа. Врши се редовна контрола система за обезбеђење, противпожарне заштите, као и инсталација за воду, струју, електронске комуникације идр. Просторије са опремом треба редовно чистити од прашине. Опрема се штити од прекида напајања.

Ако се опрема износи ради сервисирања, потребно је сачинити реверс служби обезебеђења суда у коме се наводи назив и тип опреме, серијски број и назив сервисера, који потписује руководилац службе за информатичке послове , односно лице које он овласти или лице које оваласти судска управа.

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 судске управе.

Све осетљиве и поверљиве информације у штампаном или електронском облику запослени морају одложити на сигурно место на крају радног дана или када нису присутни на свом радном месту.

Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана, осим у ситуацијама када је потребно другачије поступити, због организације посла.

Шифре за приступ не смеју бити написане и остављене на приступачном месту

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Запослени у служби за информатичке послове надзиру и проверавају 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 мора се користити опрема и подаци који су намењени тестирању и развоју.

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

Члан 20.

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 заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефиниција. Набавку антивирусног софтвера врши Министарство правде.

Употреба преносивих медија – USB меморија од стране корисника није омогућена.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса у служби за информатичке послове. 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 случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави служби за информатику и аналитику.

Судска управа и Министарство правде 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 служба за информатичке послове 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.

Корисници који комуницирају путем електронске поште (email), морају водити рачуна о могућим нападима прилоком отварања електронске поште, како не би били наведени да отворе

сумњиву електронску пошту која може садржати злонамеран прилог или линк који води до зараженог сајта или документа.

16. Заштита од губитка података

Члан 21.

Израда резевних копија базе података, корисничких и других неопходних података, ради се у служби за информатичке послове. Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

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.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

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

Инсталацију и подешавање софтвера могу да врше запослени у служби за информатичке послове.

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 службе за информатичке послове.

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.

Служба за информатичке послове предузима одговарајуће мере у циљу спречавања неовлашћеног инсталирање софтвера који може довести до угрожавања безбедности ИКТ система .

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, служба за информатичке послове је дужна да одмах примени одговарајуће активности како би се уклониле слабости и примениле мере заштите.

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 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 26.

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

Служба за информатичке послове је дужна да врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности у простору и на делу опреме, који припада само Вишем суду у Крагујевцу, који је смештен у Палати правде са другим органима. За заједничке просторије служба ће радити по налогу Министарства правде, управе Вишег суда и управника зграде.

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

Члан 27.

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 28.

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

Служба за иформатичке псолове Вишег суда у Крагујевцу задужена 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 или у управи суда.

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

Члан 29.

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 30.

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 и надзор службе за информатичке послове.

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

Члан 31.

Служба за информатичке послове Вишег суда у Крагујевцу је одговорна 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 руководилац службе 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 32.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести непосредног руководиоца, службу за информатичке послове или управу суда.

По пријему пријаве, служба за информатичке послове је дужна да одмах предузме мере у циљу заштите ресурса ИКТ система.

У зависности од врсте и значаја инцидента, руководилац службе за информатичке послове обавештава судску управу.

Одговорно лице (руководилац службе за информатичке послове - систем администратор) за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан

утицај на нарушавање информационе безбедности, поступа у складу са одговарајућом процедуром.

Служба за информатичке послове 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 33.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Вишег суда у Крагујевцу, служба за информатичке послове је дужна 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 руководилац службе за информатичке послове Вишег суда у Крагујевцу

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 34.

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 информатичке послове 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 35.

На захтев судске управе врши се провера ИКТ система.

Проверу ИКТ система врши служба за информатичке послове или лице изабрано у складу са законом којим се уређује поступак јавних набавки.

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 36.

Извештај о провери ИКТ система садржи:
1) назив оператора ИКТ система који се проверава;
2) време провере;
3) подаци о лицима која су вршила проверу;
4) извештај о спроведеним радњама провере;
5) закључке по питању усклађености Правилника о безбедности 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 37.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли и интернет страници Вишег суда у Крагујевцу.

ВИШИ СУД У КРАГУЈЕВЦУ, дана 28.03.2023. године.

Председник суда
Весна Миловановић

Служба за информатичке послове
Систем администратор