Република Србија
Основни суд у Зајечару
I-Су -1/22-76
Дана: 30.09.2022. године
З а ј е ч а р

На основу члана 52 Закона о уређењу судова („Службени гласник РС“ број 116/08, 104/09, 101/10, 31/11 - др. закон, 78/11 - др. закон, 101/11, 101/13, 106/15, 40/15-др. закон, 13/16, 108/16, 113/17, 65/18 - одлука УС, 87/18 и 88/18 - одлука УС), на основу члана 8 Закона о информационој безбедности („Службени гласник РС“ број 6/2016 и 94/17), члана 2.Уредбе о ближем садржају Правилника о безбедности информационо комуникационих система од посебног значја и садржају извештаја о провери информационог комуникационог система од посебног значаја („Службени гласник РС“ 94/2016) и члана 59. Закона о агенцији за борбу против корупције („Служебни гласник“број 94/2008, 53/2010, 66/2011, 67/2013, 8/2015),председник Основног суда у Зајечару Биљана Чолић Грајковић, дана 30.09.2022. године, допоси

ПРАВИЛНИК
ИПФОРМАЦИОНО КОМУПИКАЦИОНОГ СИСТЕМА
ОСНОВНОГ СУДА У ЗАЈЕЧАРУ

Члан 1.

Овим Правилником уређују се мере заштите од безбедоносних ризика у информационо комуникационом систему суда, начин и процедуре постизања и одржавања адекватног нивоа безбедности и овлашћења и одговорност запослених у вези безбедношћу и ресурсима ИКТ система суда.

Члан 2.

Мере прописане овим Правилником односе се на сва запослена лица, тј. на целокупно судско особље и све судије.

Члан 3.

Поједини термини у смислу овог Правилника имају следеће заначење:

1. Информационо комуникациони систем (ИКТ ситем) је технолошко организациона целина која обухвата све уређаје за електронску обраду података (хардверске и софтерске компонетне, мрежу и мрежне ресурсе, сервер и осталу комупукациону опрему);

2.Оператор ИКТ ситема је Основни суд у Зајечару, као орган јавне власти, тј. државни орган:

3.Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, да буду доступни, употребљиви на захтев овлашћених лица онда када су им потребни, да се очува изворни садржај и комплетности података, да се предупреде ризици и да се адекватно врши управљање ризицима.

4. Ризик подразумева могућност нарушавања информационе безбедности,

5.Управљање ризиком подразумева скуп мера (планирање, организовање и усмеравање активности) у циљу обезбеђења да ризици остану у прописаним и прихватљивим оквирима).

6.Инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност.

7.Мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима.

8.Тајност је својство које значи да податак није доступан неовлашћеним лицима.

9.Тајни податак је податак који је у складу са Прописима о тајности података одређен и означен одређеним степеном тајности,

10.Backup је резервна копија података:

11.UPS (UNINTERRUPTIBLE POWER SUPPLY) је уређај за непрекидно напајање електричном енергијом;

12.USB или флеш меморија је спољашни медијум за складиштење података

13.CD-ROM (COMPACT DISK-READ ONLY MEMORY) и DVD су медијуми за спимање и складиштење подаката.

14.Информациона добра обухватају пословне информације, тј. средства путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података укључујући све електронске записе, рачунарску опрему, сервер, мрежну опрему, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, интерне акте који се односе на ИКТ систем и слично.

МЕРЕ ЗАШТИТЕ

Члан 4.

Мерама заштите се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности.

Мере заштите ИКТ система обуватају следеће послове:

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

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

3.Онемогућавање, односно спречавање неовлашћене или ненамерне измене, губитака, оштећења и злоупотребе података и средстава за обраду података.

4.Заштите података и средства за обраду података од злонамерног софтвера.

5.Обезбеђење исправног и безбедног функционисање средстава за обраду података.

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

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

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

АДМИНИСТРАТОР ИКТ -СИСТЕМА

Члан 5.

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

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

Запослено лице које има администраторски налог, има право приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система) .

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

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

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

Члан 6.

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира на тај начин што се право уписују име, па презиме запосленог, која су одвојена тачком и куцају се латиничним писмом без употребе слова Ђ, Ж, Љ, Њ, Ћ, Ч, Џ, Ш.

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

Лозинка корисника мора да садржи минимум осам карактера комбинованих од малих и великих слова, цифара и специјалних знакова.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке запосленог.

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

Корисник је дужан да мења лозинку на свака два месеца.

Иста лозинка се не сме понављати у временском периоду од 6 месеци.

Члан 7.

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

Кориснички налог додељује администратор у сарадњи са непосредним руководиоцем.

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

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

НАДЗОР И КОНТРОЛА ОД СТРАНЕ АДМИНИСТРАТОРА

Члан 8.

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

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

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

ПРЕСТАНАК РАДНОГ ОДНОСА ЗАПОСЛЕНОГ И ПРОМЕНА РАДНОГ МЕСТА И ОВЛАШЋЕЊА

Члан 9.

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

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

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

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

ПРЕНОСИВИ МЕДИЈИ И АНТИРВИРУСНА ЗАШИТА

Члан 10.

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 копекцијом, имејлом, зараженим преносним медијима (USB меморијом, CD-om, идт) инсталацијом нелиценцираног софтвера и сличпо.

За успешну заштиту од вируса на сваком рачунару је инсталиран систем антивирусних дефеницја.

Забрањено је заустављање и искључивање антивирусног софтвера.

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

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

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

РЕЗЕРВНЕ КОПИЈЕ ПОДАТКА

Члан 14.

Администартор ИКТ ситема је у обавези да прави резервне копије базе података најмање једном дневно.

Базе податаја обавезно архивирају и на преносиве медије (CD Rom, DVD, USB, екстерни хард диск). За потребе обнове базе података сваки примерак преносног информатичког медија са копијама -архивама мора бити означен, бројем врстом (дневна, недељна, месечна, годишња), датумом израде копије -архиве, као и именом запосленог који је извршио копирање и архивирање.

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

Месечне копије података се чувају и ван институције-суда у случају пожара, поплава и слично.

Исправност копија-архива проверава администратор ИКТ система.

Члан 15

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

Правилник објавити и на интернет страници суда.

ПРЕДСЕДНИК
ОСНОВНОГ СУДА У ЗАЈЕЧАРУ
Биљана Чолић Трајковић