РЕПУБЛИКА СРБИЈА
ПРЕКРШАЈНИ СУД У СОМБОРУ
Број: I Су. 1-22/2013
Дана: 13. 12. 2013. године
С О М Б О Р

На основу Закона о информационом систему Републике Србије ("Службени гласник РС", бр. 12/96), Годишњег распореда послова Прекршајног суда у Сомбору I Су бр. 2-5/2013 28.11.2013. године и Правилника о унутрашњем уређењу и систематизацији радних места у Прекршајном суду у Сомбору (Су.бр. I-68/2010 од 29.07.2010.године и СУ I 1-109/2010-2 од 03.03.2011. године), вршилац функције председника Прекршајног суда у Сомбору доноси

ПРАВИЛНИК
о безбедности информација - ИТ безбедности у Прекршајном суду у Сомбору

I ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим правилником се уређује заштита и начин чувања података у оквиру информационо-комуникационих система Прекршајног суда у Сомбору, заснованих на примени рачунара, као и начин њиховог спровођења, коришћење и чување рачунарске опреме и поступак прикључивања на локалну рачунарску мрежу.

Информационо-комуникациони систем из става 1. овог члана (у даљем тексту: ИКТ систем) означава било који систем који омогућава руковање са подацима у електронском облику, а што нарочито обухвата сва средства потребна за функционисање система, укључујући рачунарске, комуникационе уређаје и инфраструктуру, софтверске ресурсе, организацију, особље и податке.

Члан 2.

Поједини изрази коришћени у овом правилнику имају следеће значење за потребе овог правилника:

- *ИТ безбедност* значи извесност да ће ИКТ систем заштити тајност, интегритет, расположивост, аутентичност и непорецивост података којима се рукује путем тог система и да ће тај систем функционисати како је предвиђено, када је предвиђено и под контролом овлашћених лица;
- *тајност* је начин поступања са податком који обезбеђује да током обраде и чувања није постао доступан неовлашћеним лицима, односно није неовлашћено обрађиван;
- *интегритет* значи очуваност изворног садржаја и комплетности податка, односно средства;
- *расположивост* је карактеристика начина управљања податком која обезбеђује да је податак доступан и употребљив на захтев овлашћених лица у тренутку када им је потребан;
- *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
- *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;

- *мере заштите* су мере које се одређују у циљу очувања информационе безбедности;

Члан 3.

Систем администратор је запослени у Прекршајном суду у Сомбору чији је задатак одржавање и унапређење заједничког рачунарског, информационог и комуникационог система, као савремена подршка раду суда.

Сиситем администратор има у својој надлежности следеће:

1. Локална рачунарска комуникациона мрежа,

2. Јавни приступ Интернету кроз рачунарску мрежу суда,

3. Интернет презентацију суда,

4. Рачунарску опрему,

5. Опрему за копирање, штампање и скенирање техничке документације,

6. Електронско архивирање података,

7. Подршка при набавци опреме и софтвера.

II ТЕХНИЧКЕ МЕРЕ ОБЕЗБЕЂИВАЊА

Члан 4.

Техничке мере обезбеђивања и заштите ИКТ система односе се нарочито на:

- физичку заштиту објекта у коме је смештена рачунарска опрема (распоред инсталација и опреме) и противпожарну заштиту;

- обезбеђивање и заштиту рачунарске опреме (избор адекватне и поуздане опреме, обезбеђивање опреме током њене експлоатације, редовно сервисирање и снабдевање резервним деловима) и рачунарских носиоца података (при коришћењу и чувању);

- заштиту програмске подршке (у фази пројектовања, развоја и коришћења програмског система);

- заштиту рачунарских мрежа (приликом пројектовања и реализације)

III ПОЈЕДИНАЧНО ПРИКЉУЧИВАЊЕ

Члан 5.

Поступак појединачног прикључивања рачунара на локалну рачунарску мрежу суда.

Појединачно прикључење корисничког рачунара на рачунарску мрежу суда, не сме ничим угрозити физички и логички интегритет рачунарске мреже. Рачунар са инсталираним оперативним системом и потребним програмима, сматра се физичким и логичким делом рачунарске мреже суда.

Само рачунар или било који други мрежни уређај, регистрован од стране Систем администратора може бити прикључен на рачунарску мрежу суда.

Члан 6.

Појединачно прикључивање корисничког рачунара искључиво спроводи Систем администратор према следећој процедури:

1. Инсталација антивирусног програма
2. Провера приступа мрежи и бази података
3. Евидентирање Провера функционалности и ауторизације оперативног система
4. Провера функционалности и конфигурације мрежне картице
5. Додељивање (TCP/IP) адресе и имена рачунара
6. прикљученог рачунара у **Евиденциони лист рачунара .**

Члан 7.

Коришћење (TCP/IP) адресе је дозвољено искључиво у контексту пословних активности Прекршајног суда у Кикинди. Додељивање (TCP/IP) адресе је у искључивој надлежности Систем администратора.

Члан 8.

Корисник прикљученог рачунара је одговоран за безбедност и интегритет података који се налазе на корисничком рачунару прикљученом на рачунарску мрежу суда.

У циљу заштите од неовлашћеног приступа рачунару прикљученог на рачунарску мрежу суда, обавезна је заштита рачунара одговарајућом лозинком и антивирусним програмом који се редовно ажурира.

Додела права приступа интерним ресурсима рачунара од стране осталих корисника мреже је у искључивој надлежности корисника. У том контексту, Систем администратор не сноси никакву одговорност у случају било ког облика неовлашћеног приступа подацима или оштећења њиховог интегритета.

Члан 9.

Сваки појединачни рачунар који је прикључен на рачунарску мрежу суда мора да поседује легалан оперативни систем и антивирусни програм.

Члан 10.

Када се из техничких (застарелост или велико оштећење) или неких других разлога, појединачно прикључени рачунар трајно искључује са мреже, Систем администратор је дужан да у року од 7 дана о томе писмено обавести одговорно лице Прекршајног суда у Сомбору **(Обавештење о трајном искључењу са мреже)**, наводећи обавезно евиденциони број рачунара.

Код непосредне замене старог рачунара новим, примењује се поступак дефинисан ставом 1 овог члана и процедура прикључивања дефинисана чланом 6. овог Правилника.

У случају поновног инсталирања оперативног система или било које друге интервенције на рачунару која је у вези са подешавањима комуникационих протокола, укључујући и промену мрежног адаптера, обавља искључиво Систем администратор уз поштовање процедуре прикључивања дефинисане чланом 6. овог Правилника.

IV МЕРЕ ЗАШТИТЕ ПОДАТАКА

Члан 11.

Прикупљени подаци могу се користити само у службене сврхе.

Државни орган који чува прикупљене податке дужан је да обезбеди брисање свих података чија је службена вредност истекла.

Члан 12.

Подаци и програмска подршка, по правилу, се чувају у два примерка, и то:

- један примерак у просторији где је смештена опрема за обраду података;
- један примерак у другој просторији органа.

Систем администратор сваког дана електронски архивира базу података Уписника Прекршај (електронско вођење уписника), а једном месечно електронски архивира пресуде-решења.

Члан 13.

Приступ подацима могу имати само овлашћена лица.

Сви запослени су одговорни за заштиту и тајност података, да правилно користе и чувају рачунарску и другу опрему.

Члан 14.

Изношење података и рачунарске опреме из просторија суда, може се вршити само по одобрењу одговорног лица.

V НАДЗОР НАД СПРОВОЂЕЊЕМ ОДРЕДБИ ПРАВИЛНИКА

Члан 15.

Унутрашњу контролу спровођења одредби овог правилника спроводи одговорно лице суда. За контролу, одговорно лице суда може да овласти и друго лице.

VI МЕРЕ У СЛУЧАЈУ НЕПОШТОВАЊА ОДРЕДБИ ОВОГ ПРАВИЛНИКА

Члан 16.

Систем администратор има ексклузивно право да без претходне сагласности одговорног лица Прекршајног суда у Сомбору, привремено укине приступ појединачног рачунара локалној мрежи или бази података, уколико процени да је то у интересу безбедности ИКТ система.

Оваква мера не може да траје дуже од 10 дана.

Члан 17.

Овај правилник ступа на снагу даном доношења.

В. Ф. ПРЕДСЕДНИКА
ПРЕКРШАЈНОГ СУДА У СОМБОРУ,
СНЕЖАНА НИКОЛАЈЕВ