**Република Србија**
**Привредни суд у Чачку**
**Су I-1/2023-45**
**08.02.2024.године**
**Ч а ч а к**

ПРИВРЕДНИ СУД У ЧАЧКУ, председник суда Зорица Миливојчевић, на основу одредби чл.52. Закона о уређењу судова („Сл. гласник РС. бр 10/2023), одредби чл.6. и 7. Судског пословника („Сл. гласник РС. бр. 110/2009, 70/2011, 19/2012, 89/2013, 96/2015, 104/2015, 113/2015, 39/2016, 56/2016, 77/2016, 16/2018, 78/2018, 43/2019, 93/2019, 18/2022), на основу члана 8. Закона о информационој безбедности („Сл. гласник РС. бр. 6/2016, 94/2017 и 77/2019), Годишњег распореда послова Привредног суда у Чачку Су I -2/2023-10 од 31.10.2023.године, Правилника о унутрашњем уређењу и систематизацији радних места у Привредном суду у Чачку Су I-1/2022-25 од 03.11.2022. године, на који је дата сагласност Министарства правде, Сектор за правосуђе број: 110-00-170/2022-03 од 21.11.2022.године, као и Плана интегритета Привредног суда у Чачку, дана 08.02.2024. године, доноси

# ПРАВИЛНИК

## о безбедности информација- ИКТ безбедности у Привредног суду у Чачку (приступ, коришћење, контрола, обнова, унутрашње опреме и др.)

## ОСНОВНЕ ОДРЕДБЕ

**Члан 1.**

Овим правилником се уређује заштита и начин чувања података у оквиру информационо-комуникационих система Привредног суда у Чачку, заснованих на примени рачунара, као и начин њиховог спровођења, коришћења и чување рачунарске опреме и поступак прикључиватња 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.

Значење појединих израза коришћених у овом правилнику је следеће:

- *Оператор ИКТ система* је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систему оквиру обављања своје делатности, односно послова из своје надлежности;
- *Информациона безбедност* представља скуп мера које омогућавају да подаци којим се рукује путем ИКТ система буду закштићени 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;
- *тајност* је својство које значи да податак није доступан неовлашћеним лицима;
- *интегритет* значи очуваност изворног садржаја и комплетност података, односно средстава
- *расположивост* је својство које значи 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 или аутентичности или непорецивости података или нарушаваиња исправног функционисања ИКТ система;
- *управљање ризиком* је систематичан скуп мера који уклучује планирање, организобвање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватливим оквирима;
- *мере заштите* ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система.

**Члан 3.**

Систем администратор је запослени у Привредном суду у Чачку чији је задатак одржавање и унапређење заједничког рачунарског, информационог и комуникационог система, као савремена подршка рада суда.

Систем 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 технипке документације
6. електронско архивирње 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 заштита рачунарске опреме (избор адекватне и поуздане опреме, обезбеђење опреме током њене експлоатације, редовно сервисирање, и снабдевање резервним деловима) и рачунарских носиоца података (при коришћењу и чувању)
- заштита програмске подршке (у фази пројектовања, развоја и коришћења програмског система)
- заштита рачунарских мрежа

## III ПОСТУПАК ПОЈЕДИНАЧНОГ ПРИКЉУЧИВАЊА РАЧУНАРА

Члан 5.

Поступак појединачног прикључивања рачунара у локалну рачунарску мрежу суда.

Појединачно прикључивање 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 по следећој процедури:

1. инсталација антивирусног програма
2. провера приступа мрежи бази података
3. евидентирање провера фунмционалности и ауторизација оперативног система
4. провера функционалности и конфигурација мрежне картице
5. додељивање (TCR/IP) адресе и имена рачунара
6. евидентирање прикљученог рачунара у евиденциони лист рачунара

Члан 7.

Коришћење (TCR/IP) адресе је дозољено искључиво у контексту пословних активности Привредног суда у Чачку. Додељивљње (TCR/IP) адресе је искључивој надлежности систем администратора.

Члан 8.

Корисник прикљученог рачунара је одговоран за безбедност и интегритет података који се налазе у корисничком рачунару прикљученом на рачунарску мрежу суда.
У циљу заштите од неовлашћеног приступа рачунару прикљученом на рачунарску мрежу суда, обавезна је заштита рачунара одговарајућом лозинком и антивирусним програмом који се редовно ажурира.

Додела приступа интерним ресурсима рачунара од стране осталих корисника мреже је у искључивој надлежности корисника, те у том контексту систем администратор не сноси никакву одговорност у случају било ког 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 разлога (застарелост или велико оштећење) или неких других разлога, појединачно прикључени рачунар трајно искључује са мреже, систем администратор је дужан да у року од 8 дана о томе писмено обавести Председника суда (обавештење о трајном искључењу са мреже), наводећи обавезно евиденциони број рачунара.

Код непосредне замене старог рачнара новим, примењује се поступак дефинисан ставом 1. овог члана и процедура прикључивања дефинисана чл.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 подтака
- један примерак у другој просторији органа

Систем администартор сваког дана електронски архивира базу података Уписника Привредног суда у Чачку (електронско вођење уписника), а једном месечно електронски архивира пресуде-решења.

Члан 13.

Приступ подацима могу имати само овлашћена лица.

Сви запослени суд одговорни за заштиту и тајност података.

Сви запослени су дужни да правилно користе и чувају рачунарску опрему 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 - Председник суда. За контролу, одговорно лице суда може да овласти и друго лице.

## VI МЕРЕ У СЛУЧАЈУ НЕПОШТОВАЊА ОДРЕДБИ ОВОГ ПРАВИЛНИКА

Систем администратор има ексклузивно право да без сагласности одговорног лица Привредног суда у Чачку, 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 16.

Овај Правилник ступа на снагу даном доношења.

Председник Привредног суда у Чачку

Зорица Миливојчевић

ДНА: - на размену података
- на от суда
- на интернет страницу суда
- систем администратору
- сектретару суда