Република Србија
ПРИВРЕДНИ СУД У ВАЉЕВУ
I Су.бр.1/2023-2
Дана 27.01.2023.год.
В а љ е в о

ПРИВРЕДНИ СУД У ВАЉЕВУ, председник суда Јасмина Игић-Матић, на основу одредби чл.52 Закона о уређењу судова, одредби чл.6 и чл.7 Судског пословника, чл.8 Закона о информационој безбедности, чл.1-8 Уредбе о ближем садржају акта о безбедности информационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја Владе РС, као и Плана интегритета Привредног суда у Ваљеву I Су.бр.1/2022-10 од 02.09.2022.год, дана 27.01.2023.год. доноси следећи

П Р А В И Л Н И К
о безбедности информација – ИТ безбедности у Привредном суду у Ваљеву
(приступ, коришћење, контрола, обнова, уништавање опреме и др)

ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим Правилником се уређује заштита и начин чувања података у оквиру информационо-комуникационих система Привредног суда у Ваљеву, 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 рачунаре, комуникационе уређаје и инфраструктуру, софтверске ресурсе, организацију, особље и податке.

Члан 2.

Значење појединих израза коришћених у овом Правилнику:

- *ИТ безбедност* значи извесност да ће ИКТ систем заштитити 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;
- *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда 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;
- *инцидент* је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система;
- *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 Ваљеву 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. локалну рачунарску комуникациону мрежу
2. јавни приступ Интернету кроз рачунарску мрежу суда
3. интернет презентацију суда
4. рачунарску опрему
5. опрему за копирање, штампање и скенирање 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 објеката 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.

Појединачно прикључивање корисничког рачунара на рачунарску мрежу суда не сме ни са чим угрозити физички и логистички 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. евидентирање прикљученог рачунара у Евиденциони лист рачунара.

Члан 7.

Коришћење (TCP/IP) адресе је дозвољено искључиво у контексту пословних активности Привредног суда у Ваљеву. 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 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 адимистратор 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 (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 рачунара 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, исту 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 суда.

Систем администратор сваког дана електронски архивира базу података Уписника Привредног суда у Ваљеву (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.

Сви запослени су дужни 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 председник суда или лице које он овласти.

VI МЕРЕ У СЛУЧАЈУ НЕПОШТОВАЊА ОДРЕДБИ ОВОГ ПРАВИЛНИКА

Члан 16.

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

Ова мера не може да траје дуже од 10 дана.

Члан 17.

Овај Правилник ступа на снагу даном доношења.

ПРЕДСЕДНИК СУДА

Јасмина Игић-Матић