Република Србија
ВИШИ СУД У СУБОТИЦИ
Су I-1 бр. 35/21-3
Датум: 22.02.2022. године
С у б о т и ц а

На основу члана 51 Закона о уређењу судова („Сл. гласник РС”, бр. 116/2008, 104/2009, 101/2010, 31/2011, 78/2011 (др. закон), 101/2011, 101/2013, 40/2015 (др. закон), 106/2015, 13/2016, 108/2016, 113/2017, 65/2018 (Одлука УС), 87/2018, 88/2018 (Одлука УС)), чл. 3 и чл. 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), председник Вишег суда у Суботици дана 22.02.2022. године доноси следећи:

П Р А В И Л Н И К
О УПРАВЉАЊУ ИНФОРМАЦИЈАМА
У ВИШЕМ СУДУ У СУБОТИЦИ

I ОПШТЕ ОДРЕДБЕ

Члан 1.

Овим правилником уређују се мере заштите података и информација (у даљем тексту: мере заштите) у Информационом систему Вишег суда у Суботици (у даљем тексту: Информациони систем-ИС) које настају у вршењу послова из надлежности Вишег суда у Суботици применом информационе технологије, као и начин њиховог спровођења.

Члан 2.

Мерама заштите штите се елементи Информационог система, а нарочито подаци, информације, програмска подршка, информатичка опрема, рачунарска мрежа и просторије у којима су смештени опрема и инсталације.

Члан 3.

Мерама заштите обезбеђују се целовитост Информационог система, аутентичност података, извора и корисника, селективан приступ и доступност подацима и другим елементима Информационог система.

Мерама из става 1. овог члана обезбеђује се заштита података и информација од случајних или намерних грешака, неовлашћеног коришћења и измена, уништења, оштећења, крађе, операционалних грешака, квара система, фалсификовања и злоупотребе података и информација у свим деловима Информационог система-ИС.

Члан 4.

Виши суд у Суботици је дужан да спроводи мере заштите у свим фазама функционисања Информационог система, од планирања, пројектовања, имплементације, експлоатације, модификације, обнављања Информационог система, до његовог гашења или конверзије на нови систем.

Члан 5.

Мере заштите могу бити организационе и техничке.

1. Организационе мере заштите

Члан 6.

Организационе мере заштите односе се на организацију заштите процеса рада и функционисања Информационог система у редовним и ванредним околностима.

Мере из става 1. овог члана односе се нарочито на:

1) одређивање одговорног лица задуженог за спровођење мера заштите у Вишем суду у Суботици у делу информационог система који се развија у области за који је надлежан Виши суд у Суботици;

2) утврђивање обавезних елемената заштите при пројектовању информационог система (подсистема) и при оперативном раду;

3) заштиту приступа подацима и заштиту од неовлашћеног коришћења података и информација;

Члан 7.

Председник Вишег суда у Суботици одређује систем администратора, као одговорно лице које је задужено за спровођење мера заштите података и информација и усмерава укупне активности на спровођењу тих мера.

Одговорно лице из става 1. овог члана предлаже и разрађује мере заштите, врши њихово евидентирање, организује спровођење тих мера и врши надзор над њиховим спровођењем.

Члан 8.

Пројекат апликације или елемената Информационог система мора да садржи, као свој саставни део, обавезне елементе заштите, као и пројектну документацију са упутством за оперативни рад за учеснике у Информационом систему и за овлашћене кориснике.

Члан 9.

Приступ подацима и информацијама у Информационом систему, као и рачунарској и комуникационој опреми могу имати само овлашћена лица.

Члан 10.

Овлашћени корисници података и информација у Информационом систему дужни су да примењују прописане мере заштите.

Заштита приступа подацима обезбеђује се провером аутентичности и идентитета овлашћеног лица на један од следећих начина:

1) на основу корисничког имена и лозинке, који се периодично морају мењати;

2) уз помоћ специјалних уређаја за препознавање отисака прстију, димензија шака, мрежњаче, гласа или физичким поређењем лика са фотографијом, у складу са техничким могућностима;

3) на основу идентификационих докумената: технологије Smart Card за проверу физичког и логичког приступа подацима и информацијама у Информационом систему у целини и појединим његовим деловима;

4) на основу других докумената (фотографија, потпис) који омогућавају утврђивање физичког идентитета овлашћеног лица за приступ и деловање у оквиру одређеног процеса и дела Информационог система.

2. Техничке мере заштите

Члан 11.

Техничке мере заштите односе се на мере обезбеђења и заштите података и информација и других елемената информационог система, које се остварују применом посебних техничко-технолошких процеса рада или спровођењем физичко-манипулативних мера заштите у било којој процедури у оквиру рада Информационог система.

Члан 12.

Мере заштите које се остварују применом посебних техничко-технолошких процеса рада могу бити хардверске и софтверске:

1) хардверске мере заштите спроводе се на специфичним информатичким уређајима за одређену врсту заштите;

2) софтверске мере заштите спроводе се путем програма или програмских пакета за одређену врсту заштите, који се извршавају на стандардној информатичкој опреми на којој се одвија апликација која се штити.

Члан 13.

Ако није могуће користити мере заштите из члана 12. овог правилника, морају се спровести адекватне физичко-манипулативне мере заштите.

Члан 14.

Техничке мере заштите подразумевају обезбеђење, евиденцију и контролу:

1) аутентичности података, њихових извора и корисника;

2) селективног приступа подацима и информацијама и осталим елементима Информационог система;

3) интегритета података израдом заштитне копије на почетку и крају сваког процеса рада и заштите архивских копија и просторија у којима се оне налазе;

4) интегритета података и информација у информационом систему у односу на појаву вируса;

5) интегритета и заштите поверљивости података применом методе криптозаштите;

6) постојећих и одређивање резервних локација, уређаја и опреме на којима ће се чувати копије база података и пројектно-програмска подршка за несметан наставак рада у случају отказивања и нарушавања редовног рада Информационог система;

7) коришћења постојећих и резервних локација, опреме и уређаја на којима ће се чувати копије база података и пројектно-програмска подршка за несметан наставак рада у случају отказивања и нарушавања редовног рада информационог система;

8) примене стандардних и посебних хигијенско-техничких мера за све елементе Информационог система, утврђене у члану 2. овог правилника, приликом њихове изградње и коришћења.

Члан 15.

Техничке мере заштите примењују се на све процесе обраде и преноса података и информација и делове Информационог система у оквиру Вишег суда у Суботици и морају бити у складу са мерама које се спроводе за Информациони систем и његову инфраструктуру у целини (рачунарска мрежа и заједнички сервер података).

II МЕРЕ ЗАШТИТЕ ПОДАТАКА

Члан 16.

Прикупљени подаци могу се користити само у службене сврхе. Виши суд у Суботици дужан је да обезбеди брисање свих података чија је службена вредност истекла.

Члан 17.

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.

У редовном оперативном раду ИС није дозвољено коришћење друге копије, осим за стварање копије за редовно коришћење.

Члан 18.

Приступ подацима могу имати само овлашћена лица. Сви приступи подацима проверавају се помоћу одговарајућих функција оперативног система.

Заштита приступа подацима обезбеђује се по нивоима, и то: путем лозинке улаза кроз систем, заштите приступа меморијама диска, заштите приступа појединим подручјима меморије диска, односно траке и заштите приступа појединим низу података.

Техничар за ИТ подршку запослен у Вишем суду у Суботици има обавезу да редовно ажурира лозинке и шифре за приступ рачунарима, најмање једном квартално.

Члан 19.

Сви приступи и трансакције са подацима и програмском подршком евидентирају се помоћу системске програмске подршке. Покушаји некоректних приступа подацима и програмској подршци сигнализирају се.

Члан 20.

Изношење података и програмске опреме из просторија Вишег суда у Суботици, односно рачунарског центра, може се вршити само по одобрењу председника суда.

Члан 21.

Заштита тајних података спроводи се поступцима селективне идентификације и ауторизације применом вишестепених, временски ограничених лозинки за улазак у систем и различитих обима овлашћења за рад са подацима.

Заштита тајних података који се због коришћења у трансакционим обрадама налазе стално на магнетним медијима са директним приступом, спроводи се применом посебних поступака и техника, а нарочито: доделом заштитних атрибута одређеним меморијским локацијама и применом криптозаштите на податке у бази података.

III МЕРЕ ОБЕЗБЕЂИВАЊА И ЗАШТИТЕ ПРОСТОРИЈА У КОЈИМА ЈЕ СМЕШТЕНА РАЧУНАРСКА ОПРЕМА

Члан 22.

Мере обезбеђивања и заштите просторија у којима су смештени рачунарска и друга информациона опрема и рачунарски центар спроводе се у складу са врстом и степеном тајности података који се обрађују и чувају у ИС.

Просторије у којима се налазе опрема и рачунски центар обезбеђују се прописаним мерама физичке заштите и противпожарне заштите.

Члан 23.

У просторијама у којима се налази рачунарска опрема могу се налазити само магнетни медији за архивирање података и програмска подршка која је потребна за непосредно обављање посла.

Члан 24.

Радне станице морају бити постављене тако да су што више удаљене од спољних зидова.

Када се ради о ИС са тајним подацима, екрани терминала, односно радних станица и штампачи морају бити тако постављени да неовлашћено лице не може видети текст који је на њима исписан.

Члан 25.

Електрична инсталација у просторијама у којима је смештена рачунарска опрема мора бити уграђена и одржавана у складу са прописима и техничким нормативима за посебну заштиту електроенергетских уређаја од пожара. Код електричне инсталације треба обезбедити заштитно уземљење свих електропроводних компонената опреме и уградити заштитни струјни прекидач.

Члан 26.

У просторијама у којима је смештена рачунарска опрема могу се налазити само они цевоводи који су неопходни за остваривање радних услова и који се на безбедном и приступачном месту могу затворити.

Члан 27.

Радници који користе рачунарску опрему морају бити оспособљени за предузимање потребних мера у случају пожара, поплаве, нестанка струје или других врста опасности.

Члан 28.

Увид у исправност рачунарске опреме и инсталација, као и увид у стање објекта у коме је смештена опрема, обезбеђује се у току 24 сата.

Члан 29.

У току и ван радног времена обезбеђује се контрола лица који улазе у просторије рачунског центра или у друге просторије у којима се налази рачунарска опрема.

Члан 30.

Под ванредним околностима, у смислу овог правилника, подразумевају се елементарне и друге веће непогоде и друге ванредне околности које могу да угрозе функционисање Информационог система - ИС. Мере за отклањање или смањивање последица изазваних ванредним околностима спроводе се у складу са планом заштите ИС у тим околностима.

IV МЕРЕ ОБЕЗБЕЂИВАЊА И ЗАШТИТЕ РАЧУНАРСКЕ ОПРЕМЕ

Члан 31.

Под рачунарском опремом, у смислу овог правилника, сматра се: систем за обраду података са периферним уређајима за уношење, архивирање и презентацију података (тастатуре, терминали, дискови, штампачи), модеми, каблови и друга информациона опрема за обраду и пренос података.

Члан 32.

Заштита рачунарске опреме врши се сагласно захтеваном нивоу заштите ИС у фази избора, експлоатације и сервисирања опреме.

Члан 33.

Приликом набавке рачунарске опреме врши се избор машинске опреме и програмске подршке која ће са високим степеном поузданости одговорити свим захтевима обраде података. При одређивању врсте и конфигурације опреме узима се у обзир нарочито: врста и степен тајности ИС, начин извршавања обраде података, обим обрада, планирани развој обрада у наредним фазама развоја ИС и могућност коришћења готових пакета за заштиту података.

Члан 34.

Приступ рачунарској опреми могу имати само овлашћена лица. Рачунарска опрема не може се користити у приватне сврхе.

V МЕРЕ ЗАШТИТЕ ПРОГРАМСКЕ ПОДРШКЕ

Члан 35.

Програмском подршком, у смислу овог правилника, сматрају се: оперативни систем, помоћни програми, развојни програми и апликативни програми.

Члан 36.

За сваки програм сачињава се програмска документација, која, нарочито, садржи: програмске поступке, изглед екрана и излазних извештаја, опис структуре података и мрежни дијаграм.

Члан 37.

Када се ради о тајним подацима, програмској документацији и апликативним програмима за рад са овим подацима одређује се врста и степен тајности, у складу са прописима о заштити тајних података.

Програми из става 1. овог члана морају бити тако израђени да се приликом исказивања података на екрану или штампачу види и врста и степен тајности података.

Члан 38.

Програмска подршка се не може неовлашћено користити, копирати и умножавати.

Приликом коришћења приватних преносних меморија (usb, cd и др.) постоји обавеза запослених у Вишем суду у Суботици да исто повере техничару за ИТ подршку.

Техничар за ИТ подршку се обавезује да онемогуће коришћење приватних преносних меморија запосленима у Вишем суду без знања и подршке ИТ техничара. Исто подразумева искључивање usb портова, cd ромова и слично.

VI МЕРЕ ЗАШТИТЕ У РАЧУНАРСКИМ МРЕЖАМА

Члан 39.

Под рачунарским мрежама, у смислу овог правилника, подразумевају се различити начини комуникационог повезивања рачунарских система: од колекције хетерогених и аутономних рачунара до групе рачунара који раде под јединственом контролом у чврстој кооперацији.

Члан 40.

Приликом пројектовања система заштите у рачунарској мрежи мора се водити рачуна о потенцијалним претњама које могу да угрозе интегритет мреже, а нарочито о: неауторизованом одливању информација, неауторизованој модификацији информација и неауторизованом одбијању коришћења мрежних ресурса.

Члан 41.

Приликом пројектовања система заштите у рачунарској мрежи мора се обезбедити нарочито: спречавање одливања садржаја порука, спречавање могућности неовлашћеног обављања анализе саобраћаја, детектовање евентуалне модификације кодираних порука, детектовање непотребног одбијања коришћења мрежних ресурса, детектовање лажних иницијалних повезивања корисника мрежних ресурса.

VII ЗАВРШНЕ ОДРЕДБЕ

Члан 42.

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

Члан 43.

Техничар за ИТ подршку запослен у Вишем суду у Суботици има обавезу да упозна све запослене у Вишем суду у Суботици са овим правилником, најкасније до 31.03.2022. године.

Члан 44.

Виши суд у Суботици ће у складу са могућностима, у зависности од преноса финансијских средстава од стране Министарства правде РС и у зависности од организовања обуке од стране Правосудне академије, Министарства правде РС или сличне институције која је уско повезана са правосуђем, омогућити најмање једном годишње едукацију запослених у ИТ сектору о новим технолошким достигнућима на пољу информационих система.

Члан 45.

Виши суд у Суботици ће у складу са могућностима, у зависности од преноса финансијских средстава од стране Министарства правде РС и у зависности од организовања обуке од стране Правосудне академије, Министарства правде РС или сличне институције која је уско повезана са правосуђем, омогућити најмање једном годишње едукацију запослених у ИТ сектору о новим међународним стандардима на пољу безбедности информација.

Члан 46.

Овај правилник ступа на снагу осмог дана од истицања на огласној табли Вишег суда у Суботици, а примењује се од 01. марта 2022. године.

ПРЕДСЕДНИК СУДА

Молнар Ференц с.р.

ЗА ТАЧНОСТ ОТПРАВКА
Одговорни радник