Република Србија
ОСНОВНИ СУД У РАШКОЈ
Су I 1-16/26
11.02.2026. године
Р а ш к а

На основу члана 12. став 1. Закона о информационој безбедности („Службени гласник РС", број 91/25), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС", број 94/16) и чл. 7 Судског пословника („Службени гласник РС“, број 110/09...и 18/22), председник Основног суда у Рашкој доноси

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ОСНОВНОГ СУДА У РАШКОЈ

I ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система Основног суда у Рашкој (у даљем тексту: Акт о безбедности), у складу са Законом о информационој безбедности („Службени гласник РС", број 91/25, у даљем тексту: Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система Основног суда у Рашкој (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2. спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;

3. подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4. прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
5. свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Акта о безбедности

Члан 3.

Мере заштите ИКТ система које су ближе уређене Актом о безбедности служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за све запослене.

Запослени у Основном суду у Рашкој морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

Запослени на пословима информатичара по уговору о делу одговоран је за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност запослених

Члан 4.

Запослени у Основном суду у Рашкој су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

Непоштовање одредби Акта о безбедности, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

Предмет заштите

Члан 5.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

II МЕРЕ ЗАШТИТЕ

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

Члан 6.

Основни суд у Рашкој у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

Интерни акти који уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу:

- Правилник о унутрашњој организацији и систематизацији радних места;
- Акт о безбедности ИКТ-а.

Сви запослени морају бити упознати са процедуром заштите безбедности ИКТ система.

Питање безбедности рада на даљину и употребе мобилних уређаја

Члан 7.

Основни суд у Рашкој не дозвољава рад на даљину ван просторија послодавца, а мобилни уређаји се не користе да се изврше одређени послови на мрежи послодавца.

Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који обављају и у потпуности разумеју своју одговорност

Члан 8.

Основни суд у Рашкој се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем, имају адекватан степен образовања и способности, као и свест о значају послова које обављају.

Основни суд у Рашкој уговором поверава активности у вези са ИКТ системом трећем лицу као пружаоцем услуга, јер у овом суду није систематизовано радно место информатичара.

Руководство Основног суда у Рашкој је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

Сви запослени у Основном суду у Рашкој су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Основни суд у Рашкој у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

- Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;
- Штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама;
- Спроводи програме заштите на конзистентан и уједначен начин у свим организационим јединицама;
- Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

Заштита од ризика који настају при променама послова или престанка радног ангажовања запослених лица

Члан 9.

Запослени и по другом основу ангажована лица дужни су да чувају поверљиве и друге информације, које су од значаја за информациону безбедност ИКТ система након престанка или промене радног ангажовања.

За поступања приликом престанка запослења или ангажовања задужена је управа суда, која предузима следеће активности:

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату,
- прегледа све налоге и приступе систему који су били доступни запосленом,
- преузима од запосленог електронске и друге уређаје,
- утврђује начин контакта са бившим запосленим након одласка,
- проверава враћене уређаје за преношење података,
- даје налог за укидање налога електронске поште и свих других права приступа систему Основног суда у Рашкој на дан престанка радног односа или другог основа ангажовања бившег запосленог,

- прегледа све налоге за приступ одлазећег запосленог и прикупља приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
- преузима картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Основног суда у Рашкој.

Дисциплински поступак

Члан 10.

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и у примени код Основног суда у Рашкој.

Дисциплински поступак покреће председник Основног суда у Рашкој, а по предлогу лица овлашћеног за праћење, прикупљање, анализу и обраду података.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Основни суд у Рашкој врши идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација. Појединци којима је дата одговорност за контролисање животног циклуса имовине дужни су да правилно управљају имовином током целог животног циклуса.

Запослени и екстерни корисници су обавезни да врате сву имовину Основног суда у Рашкој коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

Током отказног рока запослених, Основни суд у Рашкој контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности

Члан 12.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем за Основни суд у Рашкој.

Заштита носача података

Члан 13.

Основни суд у Рашкој обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података.

Запосленима је дозвољена употреба преносних носача података, односно УСБ-а, на безбедан начин, којим се своди на минимум ризик од могућег преузимања осетљивих података од стране неовлашћених особа.

Ограничење приступа подацима и средствима за обраду података

Члан 14.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности податка.

Корисницима је дозвољен приступ само мрежи и мрежним услугама за чије коришћење су овлашћени.

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Члан 15.

Основни суд у Рашкој управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Запосленима, другим радно ангажованим и екстерним корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 16.

Аутентификације корисника којима је одобрен приступ систему врши се путем јединственог корисничког имена и шифре. Сви корисници су дужни да:

- корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
- избегавају чување корисничког имена и шифре у писаном облику;
- промене шифру када примете да постоји било какав наговештај могућег компромитовања.

Шифре не заснивати на личним подацима корисника, као што су име, презиме, телефонски број или датум рођења и не смеју садржати више од 4 узастопна идентична бројчана или словна знака.

Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности, односно интегритета података

Члан 17.

Приступ ресурсима ИКТ система не захтева посебну криптозаштиту.

Запослени односно корисници користе квалификоване електронске сертификате за електронско потписивање докумената, као и аутентификацију и ауторизацију приступа појединим апликацијама.

Корисници су дужни да чувају своје квалификоване електронске сертификате како не би дошли у посед других лица.

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

Члан 18.

Основни суд у Рашкој је дужан да предузме мере ради спречавања неовлашћеног физичког приступа објекту, простору, просторијама, зони, у којима се налази ИКТ опрема, средства и документи ИКТ система, као и спречавање оштећења и ометања информација и опреме за обраду информација.

Опрема за обраду информација се штити закључавањем просторија у којима се налази и одговарајућом контролом приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава.

Безбедносне области морају бити заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ.

Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем

Члан 19.

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућности неовлашћеног приступа.

Приликом расходовања опреме потребно је претходно безбедно уколнити све осетљиве податке и лиценциране софтвере.

Правосудна стража Основног суда у Рашкој редовно прати услове околине, као што су температура и влажност, који би могли негативно да утичу на рад опреме за обраду информација.

Одржавање опреме

Члан 20.

Опрема се одржава како би се осигурали њена непрекидна расположивост и неповредивост, и то на следећи начин:

- опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;
- поправке и сервисирање опреме обавља само особље овлашћено за одржавање;
- осетљиве информације треба избрисати из опреме;
- пре враћања опреме у рад након одржавања, потребно је прегледати како би проверили да није неовлашћено коришћена или оштећена.

Измештање и премештање имовине

Члан 21.

Опрема, информације или софтвер се измештају само уз одобрење одговорног лица, а током измештања се примењују следећа правила:

- треба да се одреде запослени и спољни корисници који имају овлашћење да одобре измештање имовине;
- треба да се поставе временска ограничења за измештање опреме и да се проверава усклађеност приликом повратка.

Остављање осетљивих и поверљивих докумената и материјала

Члан 22.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

Процедура:

1. Све осетљиве и поверљиве информације у штампаном или електронском облику запослени морају одложити на сигурно место на крају радног дана или када нису присутни на свом радном месту.
2. Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана.

3. Ормари и фиоке у којима се чувају поверљиви подаци морају бити закључани када се не користе, а кључеви не смеју бити остављени на приступачном месту без надзора.
4. Лаптопови морају бити везани уз помоћ одговарајуће опреме или закључани у фиоци. Таблети и остали преносни уређаји морају бити закључани у фиоци.
5. Носачи података као што су дискови и flash меморија морају бити одложени и закључани.
6. Шифре за приступ не смеју бити написане и остављене на приступачном месту.
7. Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.
8. Материјал који је намењен за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 23.

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, дефинишу се процедуре за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевивма измештања делова ИКТ система.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 24.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен или неумрежен рачунар. Заштита од злонамерног софтвера се заснива на софтверу за откривање злонамерног софтвера и отклањање штете, на познавању информационе безбедности, као и на одговарајућим контролама приступа систему и управљању захтеваним и потребним променама.

На рачунарима у Основном суду у Рашкој инсталирана је антивирусна заштита и то програм ESET, те је потребно обезбедити његово континуирано ажурирање.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави овлашћеном лицу.

Заштита од губитка података

Члан 25.

Основни суд у Рашкој врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих и log фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Члан 26.

У ИКТ систему формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Обезбеђивање интегритета софтвера и оперативних система

Члан 27.

Основни суд у Рашкој спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за контролу промена и инсталацију софтвера, којима се обезбеђује повратак на претходно стање у случају неочекиваних ситуација на рачунарима.

Инсталацију и подешавање софтвера може да врши само радно ангажовани информатичар као овлашћено лице.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 28.

Основни суд у Рашкој врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедоносним ризицима.

Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Члан 29.

Приликом спровођења ревизије ИКТ система, Основни суд у Рашкој обезбеђује да ревизија има што мањи утицај на фукционисање система.

Основни суд у Рашкој је дужан да преко овлашћеног лица стално врши контроилни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система

Члан 30.

Заштита података који се преносе комуникационим средствима обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

Приступ садржајима на интернету је дозвољен искључиво за пословне намене.

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом.

Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 31.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, Основни суд у рашкој је у обавези да обезбеди информациону безбедност у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења.

Заштита података који се користе за потребе тестирања ИКТ система односно делова система

Члан 32.

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера наведених у овом члану.

За потребе испитивања и тестирања ИКТ система, односно делова система, Оператор ИКТ система избегава коришћење оперативних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачног добављача, купца, запосленог или др. Уколико се за сврху испитивања користе лични подаци или неке друге поверљиве информације, онда се сви осетљиви подаци и информације пре коришћења штите анонимизацијом личних података, уклањањем садржаја или изменом текста садржаја у предметном делу.

За податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су подаци о личности коришћени приликом тестирања система, одговорна су лица овлашћена за приступ и манипулацију тим подацима, у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 33.

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

Пружалац услуга је у обавези да податке, информације и документацију која му је учињена доступном користи искључиво на начин претходно одобрен од стране Оператора ИКТ система и за потребе извршења предмета уговора.

Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга

Члан 34.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, Основни суд у Рашкој успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

Уговором са пружаоцем услуга треба обезбедити могућност континуираног управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контролу безбедности информација.

Промене које се узимају у обзир су промене у споразумима са пружаоцима услуга, повећање обима текућих услуга које се нуде, као и промене које уводи Основни суд у Рашкој ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама

Члан 35.

Посебним процедурама се уређује начин одговора на инциденте нарушавања информационе безбедности и одређује особа овлашћена за контакт у случајевима нарушавања безбедности, као и контакт са надлежним органима.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени - корисник је дужан да о томе одмах обавести надређено лице, као и о уоченим и утврђеним слабостима наведеног система, и то у што краћем року, како би се инциденти нарушавања информационе безбедности спречили и како би се спречио настанак штете.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 36.

Основни суд у Рашкој примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

III ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Оператора ИКТ система

Члан 37.

Обавеза Оператора ИКТ система је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Основног суда у Рашкој.

Ступање на снагу Акта о безбедности

Члан 38.

Акт о безбедности ступа на снагу даном објављивања на огласној табли Основног суда у Рашкој.

Председник суда,

Лидија Дугалић