Република Србија
ВИШИ СУД У СОМБОРУ
Су I-1-82/2026
27.10.2026. год
С о м б о р

На основу Члана 7, 10 и 12 **Закона о информационој безбедности („Службени гласник РС“ бр. 91/25),** Члан 1-7. 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" бр.94/16**),** председница Вишег суда у Сомбору Радмила Вујин дана 27.10.2026. године, доноси

АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА У ВИШЕМ СУДУ У СОМБОРУ

I
ОСНОВНЕ ОДРЕДБЕ

Предмет правилника

Члан 1.

Актом о безбедности информационо-комуникационог система, у складу са Законом о информационој безбедности и Уредбом 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 (у даљем тексту Уредба), ближе се одређују мере заштите, принципи, начин и процедура постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Обавеза примене одредби правилника

Члан 2.

Овај Акт је обавезујући за све унутрашње организационе јединице Вишег суда у Сомбору и све кориснике информатичких ресурса овог суда, као и за сва трећа лица која користе информатичке ресурсе овог суда.

Непоштовање одредби овог Акта, као и свако угрожавање или нарушавање информационе безбедности повлачи дисциплинску одоговорност запосленог – корисника информатичких ресурса.

За праћење примене овог Акта надлежни су председник суда, секретар суда и систем-администратори Вишег суда у Сомбору.

Значење појединих термина у смислу овог правилника

Члан 3.

1. информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата:

а) електронске комуникационе мреже у смислу закона који уређује електронске комуникације

б) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;

в) податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из подтачке а) и б) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

г) организациону структуру путем које се управља ИКТ системом;

д) све типове системског и апликативног софтвера и софтверске развојне алате.

2. *оператор ИКТ система* је физичко лице у својству регистрованог субјекта, правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3.*информациона безбедност* представља способност информационо-комуникационих система и мрежа да се одупру и/или ублаже, уз одређени степен поузданости, сваки догађај који би могао да угрози расположивост, интегритет, аутентичност, непорецивост и поверљивост података који се чувају, преносе или обрађују, као и услуга које се пружају или су доступне путем тог ИКТ;

4.интегритет је својство које осигурава да подаци или информације нису промењени или уништени на неовлашћени начин од када су креирани, пренети или ускладиштени;

5. *расположивост* је својство којим се осигурава доступност и употребљивост ИКТ система на захтев овлашћеног субјекта или процеса онда када им је потребан;

6. *аутентичност* је својство којим се осигурава могућност да се провери и потврди да је информацију створио или послао онај за кога се тврди да је ту радњу извршио;

7. *поверљивост* је својство којим се осигурава да су информације и функције ИКТ система доступне само овлашћеним лицима;

8. непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

9. ризик представља могућност губитка или поремећаја изазваног инцидентом и изражава се као комбинација величине таквог губитка или поремећаја и вероватноће настанка инцидента;

10. рањивост представља слабост или недостатак у ИКТ производима или услугама који се могу искористити за реализацију једне или више претњи;

11. управљање ризиком скуп систематичних активности идентификације, процене и успостављање система контроле ризика који омогућава планирање, организовање и усмеравање мера заштите како би се обезбедило да ризици остану у прописаним и

прихватљивим оквирима;

12. избегнути инцидент представља идентификовани догађај у ИКТ систему који је могао довести до значајног угрожавања расположивости, аутентичности, интегритета, непорецивости или поверљивости података, услуга или система, али је правовременом интервенцијом или заштитним мерама спречено остваривање штетних последица;

13. претња представља сваку околност, догађај или радњу која може да угрози, поремети или на други начин штетно утиче на ИКТ систем, кориснике система и друга лица са јасном вероватноћом настајања штете у случају да изостане реакција;

14. озбиљна претња представља претњу по информациону безбедност за коју се, с обзиром на њена техничка својства, може претпоставити да има потенцијал да изазове значајне негативне последице по ИКТ систем, његовог оператора или кориснике услуга тог оператора узрокујући значајну материјалну или нематеријалну штету;

15. инцидент је сваки догађај који угрожава расположивост, интегритет, аутентичност, непорецивост или поверљивост података који се чувају, преносе или обрађују или услуге које се пружају, односно које су доступне путем ИКТ система;

16. злонамерни софтвер је софтвер намерно креиран са циљем да оштети, поремети, онемогући или неовлашћено приступи информационо-комуникационим системима и обухвата различите типове штетних програма, укључујући вирусе, тројанце, црве, рансомвер и шпијунски софтвер;

17. јединствени систем за пријем обавештења о инцидентима, је информациони систем у који се уносе подаци о инцидентима и избегнутим у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности;

18. управљање инцидентом подразумева предузимање свих радњи и поступака чији је циљ спречавање, откривање, анализа и прекид инцидента, као и предузимање других мера ради одговора на инцидент и отклањања његових последица;

19. криза информационе безбедности је догађај или стање које угрожава, омета рад или онемогућује рад ИКТ система од посебног значаја и при том изазива ризике, претње или последице по становништво, материјална добра или животну средину изузетно великог обима и интензитета које није могуће спречити или отклонити редовним деловањем надлежних органа и служби, а одговор на такав догађај или стање захтева учешће више надлежних органа, као и примену одговарајућих мера;

20. мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

21. тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

22. *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

23. безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци, као и простор или просторија која је од кључног значаја за очување информационе безбедности ИКТ система;

24. информациона добра обухватају информације које се обрађују у складу са функцијом и наменом ИКТ система; електронске записе о конфигурацији уређаја и електронске комуникационе мреже; електронске записе о интеракцијама у ИКТ системима, приступу и употреби ИКТ система (тзв. log записе); програмски кôд; техничку и корисничку документацију; електронске записе о интеракцијама у електронској комуникационој мрежи (тзв.мрежни саобраћај); информације којима се регулишу намена и коришћење ИКТ система, процеси, мере заштите и сл.;

25. пружалац управљаних услуга је субјект који пружа услуге у вези са постављањем, управљањем, радом и одржавањем ИКТ производа, мрежа, инфраструктуре, апликација или друге мреже и информационог система путем пружања помоћи или активног управљања које се спроводи у просторијама корисника услуге или на даљину;

26. податак о личности је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитеа, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуниационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета;

27. *систем назива домена (ДНС)* је дистрибуирани, хијерархијски организован систем који повезује називе домена са одговарајућим ИП адресама које се користе за усмеравање и повезивање корисничких уређаја са услугама и ресурсима на интернету;

28. пружалац услуге ДНС-а је субјекат који пружа услуге разрешавања ДНС упита корисницима интернета или пружа услугу ауторитативних сервера имена за називе домена који користе трећа лица, са изузетком коренских (енгл.root) сервера имена;

29. услуга од поверења је услуга у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

30. пружалац услуге од поверења је пружалац у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

31. квалификована услуга од поверења је услуга у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

32. пружалац квалификоване услуге од поверења је пружалац у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

33. USB или флеш меморија спољашњи медијум за складиштење података;

34. CD-ROM (Compact Disk – Read Only Memory) се користи као медијум за снимање података;

35. DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

36. Freeware је бесплатан софтвер;

37. Opensource софтвер отвореног кода;

38. Backup је резервна копија података.

Начела информационе безбедности

Члан 3.

Прилоком планирања и примене мера заштите ИКТ система треба се руководити начелима:

1. начело управљања ризиком – избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредиих околности;
2. начело свеобухватне заштите – мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система;
3. начело стручности и добре праксе – мере се примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности;
4. начело свести и оспособљености – сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесна ризика и поседују одговарајућа знања и вештине;
5. начело континуираног побољшања – мере заштите и управљања информационом безбедношћу треба редовно процењивати и унапређивати како би се осигурала њихова ефикасност и прилагодљивост новим претњама и технолошким променама;
6. начело равноправности недискриминације – мере заштите ИКТ система морају се спроводити на начин који осигурава једнак третман свих корисника, без дискриминације по било ком основу, у складу са законом.

Обрада података о личности

Члан 4.

На обраду података о личности која неопходна за вршење и испуњење обавеза из овог закона примењују се одредбе овог закона, одредбе посебних закона којима се уређују одређене области, као и одредбе закона којим се уређује заштита података о личности.

II
МЕРЕ ЗАШТИТЕ

Члан 5.

Мерама заштите обезбеђује се превенција од настанка инцидената који угрожавају обављање делатности Вишег суда у Сомбору, односно превенција и смањење штете

од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима

Са садржином овог Акта биће упознати сви запослени овог суда и дужни су да поступају у складу са одредбама овог Акта, као и других интерних процедура које регулишу информациону безбедност.

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

Мере заштите систематизоване су у 37 тачака прописаних Чланом 10. став 4. Закона о ииформационој безбедности, уз опис процедура, овлашћења и одговорности учесника у спровођењу сваке мере, при чему ће изричито бити напоменуто уколико одређена мера заштите прописана Чланом 10. став 4. Закона о информационој безбедности није примењива на Виши суд у Сомбору.

Мере заштите ИКТ система се односе на:

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

Сваки запослени-корисник ресурса ИКТ система одговоран је за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности.

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система суда надлежни су систем-администратори Вишег суда у Сомбору, у склопу послова свог радног места прописаних Правилником о унутрашњем уређењу и систематизацији радних места у Вишем суду у Сомбору.

5.2) Прикупљање података о претњама по информациону безбедност ИКТ система

Систем-администратори прикупљају податке о претњама по информациону безбедност ИКТ система из антивирусног програма.

Подаци се прикупљају свакодневно односно одмах по утврђењу претње од стране антивирусног програма, док систем-администратори Вишег суда у Сомбору за наведене околности шаљу годишњи извештај ЦЕРТ-у.

5.3) Постизање безбедности рада на даљину и употребе мобилних уређаја

Рад на даљину и употреба мобилних уређаја у ИКТ систему није могућа.

5.4.) Обезбеђивање оспособљености корисника и управљача ИКТ системом, одржавање обука за све руководиоце, запослене и ангажована лица која имају приступ ИКТ системима

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места. Виши суд у Сомбору се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о о значају послова које обављају.

Систем-администратори Вишег суда у Сомбору су дужни да сваког корисника ИКТ ресурса, одмах по заснивању радног односа, упознају са одговорностима и правилима коришћења ИКТ ресурса Вишег суда у Сомбору.

Свако коришћење ИКТ ресурса Вишег суда у Сомбору од стране запосленог-корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог.

5.5) Обезбеђивање довољно ресурса за адекватно управљање информационом безбедношћу

Министарство правде обезбеђује антивирусне програме које суд користи у свом раду, те обезбеђује њихово редовно ажурирање.

Виши суд у Сомбору ће у свом редовном организационом и финансијском пословању, а у сарадњи са систем-администраторима, у склопу планирања финаисијских средстава за сваку годину, у случају утврђења такве потребе, предвиђати и финансијска средства ради обезбеђивања довољних физичких и техничких ресурса за адекватно управљање информационом безбедношћу, исказивањем потреба Министарству правде у редовном буџетском планирању.

5.6) Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

У случају промене послова или надлежности корисника-запосленог, систем-администратори ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а у складу са новим пословима корисника-запосленог.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида.

О престанку радног односа или ангажовања као и о промени радног места систем-администратори су дужан да се информишу у судској управи суда ради укидања, односно измене приступних привилегија за наведеног запосленог-корисника.

Корисник ИКТ ресурса, након престанка радног ангажовања у суду, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

5.7) Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Информациона добра обухватају све информације које Виши суд у Сомбору обрађује у складу са функцијом и наменом ИКТ система, електронске записе о конфигурацији уређаја и електронске комуникационе мреже, електронске записе о интеракцијама у ИКТ системима, приступу и употреби ИКТ система (тзв.log записе), програмски код, техничку и корисничку документацију, електронске записе о интеракцијама у електронској комуникационој мрежи (тзв. мрежни саобраћај), информације којима се регулише намена и коришћење ИКТ система, процеси, мере заштите и сл.

Евиденцију о информационим добрима воде систем-администратори у папирној или електронској форми.

5.8) Класификовање нивоа заштите података према значају, у складу са начелом управљања ризиком

Подаци који се налазе у ИКТ систему представљају пословну тајну и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима ("Сл.гласник РС" бр.53/11).

5.9) Заштита носача података

Оператор ИКТ система обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја које се чувају на носачима података.

Подаци могу да се сниме (архивирају или запишу) на серверу на ком се снимају подаци, у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право омогућено.

Подаци и документи могу да се сниме на друге носаче (специјални уређаји за смештање података тзв. „*storage*“, екстерни хард диск, УСБ, ЦД, ДВД) само од стране овлашћених запослених-корисника.

Носачи информација морају бити прописно обележени и одложени на место на ком ће бити заштићени од неовлашћеног приступа. У случају транспорта носача информација председник суда, уз консултацију систем-администратора, одредиће одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на носачима, подаци морају бити трајно обрисани, а уколико то није могуће, такви носачи морају бити физички оштећени односно уништени, ради онемогућавања приступа таквим подацима.

5.10) Ограничење приступа подацима и средствима за обраду података

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има.

Запослени који има администраторски налог има право приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталација, одржавања, подешавања и управљања ресурсима ИКТ система.

Запослени-корисник може да користи само свој кориснички налог који је добио од администратора и не сме омогућити другом лицу коришћење његовог корисничког налога, сем администратору ради подешавања корисничког профила и радне станице.

Запослени-корисник који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.

Запослени-корисник дужан је да поштује и следећа правила безбедног и примерног коришћења ресурса ИКТ система и то да:

- користи информатичке ресурсе искључиво у пословне сврхе
- прихвати да су сви подаци који се складиште, преносе или процесуирају у оквиру информатичких ресурса власништво Вишег суда у Сомбору и да могу бити прегелд надгледања или прегледања
- поступа са поверљивим подацима у складу са прописима, а посебно при копирању и преносу података
- безбедно чува своје лозинке, односно исте не одаје другим лицима изузев у случају нужде и потребе хитног приступа његовој радној станици
- мења лозинке сагласно утврђеним правилима
- пре сваког удаљавања од радне станице одјави се са система, односн закључа радну станицу
- обезбеди сигурност података у складу са важећим прописима
- приступа информатичким ресурсима само на основу експлицитно додељених корисничких права
- не зауставља рад и не брише антивирусни програм, не мења његове подешене опције, нити неовлашћено инсталира други антивирусни програм
- не сме на радној станици складиштити садржај који не служи у пословне сврхе
- користи интернет и електронску пошту у складу са прописаним процедурама
- прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности
- прихвати да технике сигурности (антивирус програми, firewall системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др) спречавају потенцијалне претње ИКТ систему
- не сме инсталирати, модификовати, искључити из рада или брисати заштитни, системски или апликативни софтвер

5.11) Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему

Право приступа имају само запослени-корисници који имају администраторске или корисничке налоге.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Администраторски налог може да користи искључиво систем-администратор Вишег суда у Сомбору.

Кориснички налог се састоји од корисничког имена и лозинке на основу којих се врши аутентификација-провера идентита и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника. Кориснички налог додељује администратор, на основу захтева судске управе, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратори воде евиденцију о корисничким налозима, проверавају њихово коришћење, мењају права приступа и укидају корисничке налоге на основу захтева запосленог на пословима управљања људским ресурсима, односно надлежног руководиоца.

Сви запослени Вишег суда у Сомбору имају приступ ИТ систему Вишег суда у Сомбору, али се морају придржавати следећих правила у вези свог корисинчког налога како би се заштитила безбедност мреже, интегритет података и система у целини:

- Сваки запослени у суду има своје индивидуално корисничко име, као и шифру за приступ ИТ систему Вишег суда у Сомбору, те за програм аутоматског вођења предмета.
- Приступне шифре за електронску базу прописа и судских одлука доставиће се на захтев запосленог, а по одобрењу од стране судске управе.
- Све шифре имају следећа подешавања: Минимални број карактера је 12, шифру чини комбинација алфабетских и нумеричких знакова, великих и малих слова. Шифра за приступ ИТ систему се мења на сваких 60 дана.
- Корисничке шифре не треба да буду сачињене тако да садрже лично име запосленог.
- Захтев за нови налог рачунара или корисника, као и брисање постојећег налога, мора бити формално ауторизован од стране судске управе. Судска управа је дужна обавештавати систем-администраторе о променама запослених у суду како би списак запослених са корисничким именом био ажуран, те по пријему обавештења о промени запослених, систем-администратори су у обавези да у што краћем року направе или обришу корисничко име.

5.12) Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Аутентификација корисника коме је одобрен приступ систему врши се путем јединственог корисничког имена и лозинке. Корисници су дужни да своје корисничко име и лозинку држе у тајности и не откривају другим лицим а укључујући и надређене особе, изузев у слулају нужде и потребе хитног приступа његовој радној станици. Потребно је избегавати чување корисничког имена и лозинке у писаном облику.

Ако запослени-корисник посумња да је друго лице открило његову лозинку или да је лозинка на било који начин компромитована дужан је да исту одмах измени.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве или лако утврдиве податке.

5.13) Предвиђање употребе криптографских контрола и других техника за сакривање података ради заштите поверљивости, аутентичности и интегритета података

Приступ ИКТ ресурсима Вишег суда у Сомбору не захтева криптозаштиту.

5.14) Примена мера заштите ради спречавања отицања података

Запосленима Вишег суда у Сомбору је забрањено свако неовлашћено коришћење података мимо њихове употребе искључиво у службене сврхе, као и дељење и одлив података ван ИКТ система Вишег суда у Сомбору.

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

Виши суд у Сомбору је обавезан да предузме мере ради спречавања неовлашћеног физичког приступа сервер сали, активној и пасивној мрежној опреми, као и другим просторијама у којима се налази ИКТ опрема, средства и документи ИКТ система као и спречавање оштећења и ометање информација.

Простор у коме се налазе сервери, мрежна и комуникациона опрема ИКТ система, организован је као административна зона. Наведени простор мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, снабдевен адекватном климатизацијом ради одржавања одговарајуће температуре, уз забрањен приступ незапосленим и неовлашћеним лицима.

Да би приступила сервер сали Вишег суда у Сомбору, трећа лица морају добити одобрење систем-администратора Вишег суда у Сомбору, те трећа лица којима је одобрен приступ сервер сали у исту могу приступити само уз присуство овлашћеног лица.

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

Улаз у просторије у којима се налази ИКТ опрема дозвољен је само администратору ИКТ система и запосленим-корисницима ИКТ система. Изузев администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, уз присуство надлежног лица, као и лица која пружају услуге одржавања хигијене, уз присуство надлежног лица.

Административна зона мора имати противпожарну опрему која се користи само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима. Сервер соба мора бити опремљена детектором дима и пожара, који треба да се подеси на аутоматски рад, и која опрема за детекцију мора бити тестирана најмање једном годишње.

Сваки сервер у Вишем суду у Сомбору мора бити прикључен на свој одговарајући УПС генератор, који би га штитио од осцилација напонске мреже, као и штитио податке одређено време у случају нестанка електричне енергије, који УПС генератор мора бити тестиран најмање једном годишње.

Сервери и активна мрежна опрема (switch, модем, router, firewall) морају стално бтии прикључени на уређаје за непрекидно напајање електричном енергијом – УПС. У случају нестанка електричне енергије у периоду дужем од капацитета УПС-а, овлашћно лице дужно је да искључи опрему у складу са процедурама произвођача опреме. ИКТ опрема се у случају опасности (пожар, временске непогоде и сл), може изнети и без одобрења председника суда.

Опрема се одржава како би се осигурали њена непрекидна расположивост и неповредивост у складу са препорученим сервисним интервалима према спецификацијама које је дао испоручилац. Поправке и сервисирање опреме обавља само особље овлашћено за одржавање.

У случају изношења опреме ради селидбе или сервисирања, неопходно је одобрење председника суда који ће одредити услове, начин и место изношења опреме. Ако се опрема износи ради сервисирања, поред одобрења председника суда, систем администратор је дужан да сачини записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, и кратак опис квара. Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Вишег суда у Сомбору.

5.17) Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Систем-администратори континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и у складу с тим планирају, односно предлажу одговарајуће мере.

Пре увођења у рад новог софтвера неопходно је направити копију архиве постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију.

Инсталирање новог софтвера, као и ажурирање постојећег односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запослених-корисника. У случају да се на новој верзији софтвера који је уведен у рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

5.18) Примена процедура и мера заштите приликом коришћења услуге рачунарства у клауду

ИКТ систем Вишег суда у Сомбору не користи услуге рачунарства у „cloud“-у.

5.19) Праћење ИКТ система у циљу откривања рањивости и претњи

Систем-администратори су дужни да поступају по свим обавезним упутствима и процедурама Министарства правде прописаним у циљу откривања рањивости и претњи, те да о истима благовремено упознаје запослене и обезбеђује њихову примену.

У случају открића да се одређени запослени не придржава обавезних мера заштите, односно да излаже ИКТ систем Вишег суда у Сомбору рањивостима или претњама, дужни су да га најпре опомену и, уколико је то могуће, отклоне рањивост или претњу. Уколико запослени не поступи по упозорењу систем-администратора, односно понови поступање које излаже ИКТ систем рањивости или претњи, систем администратори ће о томе без одлагања обавестити судску управу ради доношења одлуке о покретању дисциплинског поступка.

У случају утврђивања одређене рањивости или претње по ИКТ систем, а која није претходно утврђена или евидентирана од стране Министарства правде, систем администратор ће о томе обавестити Министарство правде ради предузимања даљих мера заштите.

5.20) Ограничење приступа веб презентацијама које могу потенцијално да наруше безбедност ИКТ система

Било какав покушај запосленог за приступ веб презентацијама које потенцијално могу да наруше безбедност ИКТ система је строго забрањен.

Веб презентације којима је омогућен приступ од стране корисника ИКТ система су унапред одређене и дефинисане од стране Министарства правде и приступ другим веб презентацијама није омогућен.

У случају да приликом приступа на поједину веб презентацију запослени посумња или добије обавештење да приступ појединој веб презентацији може бити штетан, дужан је обустави даљи приступ презентацији и контактира систем-администратора, који ће потом утврдити да ли је приступ наведеној презентацији дозвољен.

5.21) Заштита података и средстава за обраду података од злонамерног софтвера

Заштита од злонамерног софтвера на мрежи се спроводи у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносинм медијима (УСБ меморија, ЦД итд), инсталацијом нелиценцираног софтвера и сл.

За заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефиниција. Набавку антивирусног софтвера врши Министарство правде.

Употреба преносивих медија – УСБ меморија од стране корисника није омогућена, изузев на рачунарима систем-администраториа и секретара суда.

Преносиви медији, пре коришћења морају бити проверени на присуство вируса од стране систем-администраториа. Ако се утврди да преносиви медиј садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером. Ризик од евентуалног губитка података приликом чишћења медија од вируса сноси доносилац медија.

У случају да корисник примети необично понашање рачунара, потребно је да наведено без одлагања пријави систем-администраторима.

Запосленим-корисницима који су прикључени на ИКТ систем строго је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема) као и недозвољена употреба интернета која обухвата:

- нарушавање сигурности мреже или друго онемогућавање пословне интернет комуникације
- намерно ширрење деструктивних и опструктивиних програма на интернету (интернет вируси, тројански коњи, црви и друге врсте малициозног софтвера)
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено
- преузимање (download) података знатне величине, који проузрокује оптерећење мреже
- преузимање (download) софтвера и материјала заштићених ауторским правима
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видео стриминг и др)
- недозвољен приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета

У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

- службени налози за електронску пошту могу се користити искључиво за службену комуникацију, пријављивањем на сервисе из оквира пословног окружења, док се исти не смеју користити за личну комуникацију, прослеђивање ланчаних порука, за пријаве на сервисе електронског банкарства, комуналних услуга и у друге приватне потребе)
- електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса већ се мора избрисати или пријавити систем администратору
- не смеју се попуњавати нити слати подаци као што су корисничко име, лозинка, бр. телефона, алтернативна адреса електронске поште и слично уколико се исти траже путем мејла, јер су у питању покушаји злоупотреба
- не прихватати опције за покретање неког другог програма/апликације, уколико се при отварању документа из прилога појави порука типа "ок/сагласан".

5.22) Заштита од губитка података редовном израдом резервних копија података

Виши суд у Сомбору врши израду резервних копија података који обухватају системске информације и податке неопходне за опоравак система у случају наступања последица изазваних ванредним околностима. Од губитка података се обезбеђује креирањем резервних копија података на специјалним серверима за складиштење података.

Систем-администратори праве редовне дневне, недељне и месечне резервне копије система за аутоматско вођење предмета (АВП) и базе података.

Систем-администратори ће правити резервне копије свих осталих релевантних података корисника.

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

О акитвностима администраотра и запослених-корисника воде се дневници активности (activity log, security log, transaction log и др)

О догађајима који могу бити од значаја за безбедност ИКТ система води се регистрација и евидентирање кроз систем анитвирусне заштите и извештаји се једном годишње достављају Националном ЦЕРТ-у.

5.24) Обезбеђивање интегритета софтвера и оперативних система

У ИКТ систему може да се инсталира искључиво софтвер за који постоји важећа лиценца у власништву Министарства правде или Вишег суда у Сомбору или Freeware Opensource верзије.

Инсталацију и подешавање софтвера врши систем-администратори Вишег суда у Сомбору.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера, уз присуство систем-администратора Вишег суда у Сомбору.

Пре сваке инсталације нове верзије софтвера, односно подешавања, неопходно је направити копију постојећег како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

5.25) Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Систем-администратори предузимају одговарајуће мере у циљу спречавања неовлашћеног инсталирања софтвера који може довести до угрожавања безбедности ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, систем-администратори су дужни да одмах примене одговарајуће активности како би се уклониле слабости и примениле мере заштите.

Подешавањем корисничких полиса од стране систем-администратора онемогућено је инсталирање софтвера који може довести до угрожавање безбедности ИКТ система

5.26) Обезбеђивање заштите ИКТ система приликом спровођења ревизорског тестирања

Приликом вршења ревизије ИКТ система потребно је исту вршити на начин да се оствари што мањи утицај на редовно фукционисање система. Уколико се током ревизије оствари већи утицај на функционисање система, потребно је одговарајуће поступке прекинути или одложити.

У случају утврђења иregуларности или неусклађености ИКТ система приликом вршења ревизије, систем-администратори одмах, а најкасније у року од 3 месеца спроводи мере за отклањање утврђених иregуларности. У случају да систем-администратори није у могућности да самостално отклони утврђене иregуларности и неусклађености, о истима обавештава одговарајући сектор Министарства правде ради пружања подршке.

Екстерна ИКТ ревизија се не спроводи.

5.27) Заштита података у комуникационим мрежама, укључујући уређаје и водове

Комуникациони каблови и каблови за напајање постављени су тако да се обезбеди изолација од могућих спољашњих оштећења, постављањем истих, где год је то могуће, у зид или каналице, на начин да се онемогући неовлашћен приступ односно изврши изолација од могућих оштећења.

Систем администратори су дужни да врше контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалних неправилности у простору и на делу опреме.

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

Размена података са државним органима, правним и физичим лицима се врши у складу са важећим прописима и унапред дефинисаним потписаним уговорима.

5.29) Испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Инсталирање нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Вишем суду у Сомбору дефинише се уговором закљученим са наведеним лицима.

Систем-администратори Вишег суда у Сомбору задужени су за технички надзор над реализацијом уговорених обавеза од стране трећих лица. Документација, упутства и процедуре добијене од стране трећих лица при инсталацији или замени ресурса ИКТ система чувају се у службеним просторијама систем-администратора или судске управе.

5.30) Заштита података који се користе за потребе тестирања ИКТ система

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 упоредила актуелна и очекивана понашања.

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

За потребе испитивања и тестирања ИКТ система, односно делова система, Виши суд у Сомбору 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 потребе тестирања ИКТ система односно делова система систем-администратори суда могу да користе податке који нису осетљиви, а које штите, чувају и контролишу на одговарајући начин.

5.31) Процедуре за чување и брисање информација у ИКТ системима

Описане процедуре биће накнадно утврђене након доношења новог подзаконског акта, у смилсу Члан 54. Закона о информационој безбедности, а којим се ближе уређује садржина акта о информационој безбедности односно ближе уређују мере заштите ИКТ система прописане Члан 10. Закона о информационој безбедности.

5.32) Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Трећа лица – пружаоци услуга израде и одржавања софтвера могу приступити само софтверу који су они израдили и подацима који нису осетљиви. За пружаоце

услуга нужно је да постоји уговором дефинисан приступ уз контролу и надзор службе за информатичке послове и уговор о поверљивости.

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

Систем-администратори Вишег суда у Сомбору одговорни су за надзор над поштовањем уговорених обавеза од стране трећих лица – пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система. У случају непоштовања уговорних обавеза систем-администратори су дужни да одмах обавесте судску управу.

5.34) Превенција и реаговање на безбедносне инциденте, уз адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама и примену мера санације последица инцидента;

Поступање по овој мере детаљније је описано у тачки 19. мера заштите овог Акта.

5.35) Мере које обезбеђују континуитет обављања посла у ванредним околностима

У случају ванредних околности које могу да доведу до измештања ИКТ система из зграде Вишег суда у Сомбору, систем администратори су дужни да по налогу судске управе у најкраћем року пренесу делове ИКТ неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама одређују систем-администратори Вишег суда у Сомбору,

Делови ИКТ система који нису неопходни за функционисање у ванредним ситуацијима, складиште се на резервну локацију коју одреди председник суда.

Складиштење делова ИКТ система који нису неопходни врши се на начин да опрема буде безбедна и обележена у складу са евиденцијом која се о њој води.

5.36) Усвајање докумената којима се дефинишу процедуре за проверу адекватности мера заштите;

Описана мера биће накнадно утврђена након доношења новог подзаконског акта, у смилсу Члан 54. Закона о информационој безбедности, а којим се ближе уређује садржина акта о информационој безбедности односно ближе уређују мере заштите ИКТ система прописане Члан 10. Закона о информационој безбедности.

5.37) Употреба мултифакторске аутентификације или решења континуиране провере аутентичности, заштићене гласовне, видео и текстуалне комуникације, те безбедних комуникационих система у хитним случајевима унутар оператора ИКТ система.

Наведена мера заштите није примењива за Виши суд у Сомбору, у ком се не примењује мултифакторска аутентификација нити заштићене гласовне, видео и текстуалне комуникације, нити је њихвоа употреба прописана од стране Министарства правде.

III
ИЗМЕНЕ АКТА О БЕЗБЕДНОСТИ

Члан 6.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедности, систем-администратори дужан је да обавести судску управу, како би се приступило измени овог Акта, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивања овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IV
ПРОВЕРА АКТА О О БЕЗБЕДНОСТИ

Члан 7.

Провера ИКТ система врши се на захтев судске управе, а најмање једном годишње.

Проверу ИКТ система врши систем-администратори Вишег суда у Сомбору или лице изабрано у складу са Законом којим се уређује поступак јавних набавки.

Провера се врши тако што се:

1. проверава усклађеност Акта о безбедности информационог система, узимајући у обзир Правилнике на које се врши упућивање, са прописаним условима, односно провером да ли су Актом адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему
2. проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима
3. врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове), као и методом тестирања постојања безбедносних слабости у сличним окружењима.

О извршеној провери сачињава се извештај који се доставља судској управи.

Члан 8.

Извештај о провери ИКТ система садржи:

1. назив оператора ИКТ система који се проверава
2. време провере
3. податке о лицима која су вршила проверу
4. извештај о спроведеним радњама провере
5. закључак по питању безбедности Акта о безбедности ИКТ система са прописаним условима
6. закључке по питању адекватне примене предвиђених мера заштите у оперативном раду
7. закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система
8. оцена укупног нивоа информационе безбедности
9. предлог евентуалних корективних мера
10. потпис одговорног лица које је спровело проверу ИКТ система

V
ИЗВЕШТАВАЊЕ О ИНЦИДЕНТИМА

Члан 9.

Систем-администратори Вишег суда у Сомбору дужни су да доставе обавештење о инциденту који може да има значајан утицај на нарушавање информационе безбедности, без одлагања, а најкасније у року од 24 сата од када су сазнали за инцидент.

Инциденти који могу да имају значајан утицај на нарушавање информационе безбедности су:

1 инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга

2. инциденти који утичу на велики број корисника услуга или трају дужи временски период

3. инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружању услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност.

4. инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије

5. инциденти који доводе до неовлашћеног приступа подацима чије откривање може угрозити права и интересе оних на које се подаци односе

6. инциденти који изазивају или могу да изазову знатну материјалну или нематеријалну штету оператору ИКТ система од посебног значаја и другим физичким и правним лицима.

Систем-администратори Вишег суда у Сомбору дужни су да пријаве и избегнуте инциденте који представљају озбиљну претњу и који би могли довести до околности сличних онима описаним у ставу 2. овог члана. У случају инцидената у ИКТ системима за рад са тајним подацима оператори тих ИКТ система поступају у складу са прописима којима се уређује област заштите тајних података.

Достављање обавештења о инцидентима

Члан 10.

Систем-администратори Вишег суда у Сомбору дужни су да обавештења о инцидентима доставе у јединствени систем за пријем обавештења о инцидентима путем веб презентације Министарства или Канцеларије за информациону безбедност.

Систем-администратори Вишег суда у Сомбору дужни су да путем одговарајућих канала комуникације обавесте о инциденту кориснике којима овај суд пружа услуге, без одлагања, у случају инцидента који може да изазове или изазива штетан утицај на пружање и коришћење услуга, као и о мерама које корисници могу да предузму и употребе у циљу умањења или елиминације штетних последица инцидената.

Обавештење о инциденту мора да садржи:

1 податке о подносиоцу пријаве

2. врсту и опис инцидента и процену да ли је инцидент последица кривичног дела

3. датум и време почетка инцидента, односно сазнања о инциденту и трајање инцидента

4. последице које је инцидент изазвао

5. предузете активности ради ублажавања последица инцидента

6. иницијалну процену нивоа опасности и утицаја инцидента на ИКТ систем, као и индикатора компромитације

7. информацију о евентуалном прекограничном дејству инцидента

8. податке о претходно пријављеним сличним инцидентима ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете

9. друге релевантне инфомрације по потреби

Извештавање током и након инцидента

Члан 11.

Систем-администратори Вишег суда у Сомбору дужни су да:

1. достављају извештај о инциденту током трајања инцидента, са описом мера које су преузете за решавање инцидента, у јединствени систем за пријем обавештења о инцидентима и то:

- на свака три дана у случају инцидента средњег нивоа
- на свака 24 сата у случају инцидената високог и веома високог нивоа

2. достављају обавештења и додатне извештаје о битним догађајима у вези са инцидентом и активностима које предузима, на захтев Канцеларије за информациону безбедност

3. достављају завршни извештај о инциденту у року од 15 дана од дана престанка инцидента који садржи следеће податке:

а. врсту и детаљан опис инцидента

б. врсту претње и узрок који је довео до инцидента

в. време и трајање инцидента

г. обим и степен утицаја инцидента (остварени ризик), односно последице које је инцидент изазвао

д. информацију о евентуалном прекограничном дејству инцидента

ђ. предузете активности ради отклањања последица инцидента и, по потреби, друге информације од значаја за евидентирање инцидента и статистичку обраду.

Достављање статистичких података о инцидентима

Члан 12.

Систем-администратори Вишег суда у Сомбору дужни су да, поред обавештавања о инцидентима који значајно нарушавају информациону безбедност, доставе органу, односно организацији надлежној за послове Националног ЦЕРТ-а, статистичке податке о свим инцидентима у ИКТ систему, укључујући и избегнуте инциденте, у претходној години најкасније до 28. фебруара текуће године.

Виши суд у Сомбору извештај о статистичким подацима доставља Министарству и објављује на веб презентацији Вишег суда у Сомбору.

Врста, форма и начин достављања статистичких података из става 1. овог члана утврђује орган, односно организације надлежна за послове Националног ЦЕРТ-а.

VI
ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Овај Акт ступа на снагу осмог дана од дана објављивања на огласној табли и интернет страници Вишег суда у Сомбору.

ПРЕДСЕДНИЦА СУДА
РАДМИЛА ВУЛИН