РЕПУБЛИКА СРБИЈА
ВИШИ СУД У НИШУ
Су I-1 бр. 12/22

# АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНИХ СИСТЕМА ВИШЕГ СУДА У НИШУ

На основу члана 8. Закона о информационој безбедности ( „Службени гласник Р.С.број 6/16, 94/17 и 77/19), чланова 1-8 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, Владе РС ("Службени гласник РС", број 94/16 од 24.11.2016. године) , а у вези са судским пословником председник Вишег суда суда у Нишу Драгана Живадиновић доноси:

**АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНИХ СИСТЕМА ВИШЕГ СУДА У НИШУ**

## I. Уводне одредбе

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности(„Службени гласник РС“, број 6/16, 94/17 и 77/19) и Уредбом о ближем садржају правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештја о провери безбедности информационо-комуникационих система од посебног значаја („Сл. Гласник РС“, бр. 94/2016), утврђују се мере заштите а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информационо- комуникационих система (у даљем тексту ИКТ систем).

Члан 2.

**Циљеви доношења овог Правилника су:**

- допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
- минимизација безбедносних инцидената;
- допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистентне контроле свих компонената ИКТ система

Акт о безбедности информационих-комуникационих система Вишег суда представља скуп потребних предуслова и правила таквих да би се обезбедило неометано функционисање ИКТ система Вишег суда, и рад самог корисника као и да би се смањили ризици од „непожељних догађаја“. Акт о безбедности треба још да обезбеди поверљивост, интегритет али и доступност информацијама који се налазе у ИКТ систему Вишег суда.

Акт о безбедности информационих система Вишег суда покрива питања везана за коришћење Интернета, електронске поште, АВП програма, поверљивости информација, личне употребе система, српског законодавства, физичке безбедности ИТ система као и лиценцирања софтвера.

Разлог увођења овог Акта о безбедности је покушај да се смање потенцијалне претње ИКТ систему Вишег суда, међутим не искључује се могућност да се и поред ових заштитних мера неки „непожељни догађаји“ и даље десе. Ако се то и догоди, треба открити узрок како је до инцидента дошло, отклонити га и када се узрок утврди у Акту о безбедности треба уврстити и поступак који би смањио ризик да до истог инцидента поново не дође.

Члан 3.

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

Непоштовање одредби овог правилника као и свако угрожавање или нарушавање информационе безбедности повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса.

За праћење примене овог правилника надлежан је председник суда, секретар суда и информатичари Вишег суда у Нишу.

Члан 4.

Поједини појмови у смислу овог правилника имају следеће значење:

1. информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата све уређаје за електронску обраду података (хардверске и софтверске компоненте, мрежу и мрежне ресурсе, сервер и осталу комуникациону опрему);
2. оператор ИКТ система је Виши суд у Нишу као орган јавне власти тј. државни орган;
3. информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;
4. тајност је својство које значи да податак није доступан неовлашћеним лицима;
5. интегритет значи очуваност изворног садржаја и комплетности података;
6. расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
7. аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
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 значи могућност нарушавања инфомиационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
10. 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;
11. инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
12. мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
13. тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одговарајућим степеном тајности;
14. информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

15. VPN (Virtual Private Network) је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
16. WAN (Wide Area Network) је мрежа широког подручја која покрива веће подручје (градове, државе или континенте) и обично се користи за међусобно повезивање удаљених рачунара или локалних (LAN) мрежа.
17. Backup је резервна копија података;
18. Download је трансфер података са централног рачунара или web презентације на локални рачунар;
19. MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
20. UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
21. Firewall је „заштитни зид" односно систем преко кога се врши надзор и контролише проток инфоимација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
22. USB или флеш меморија је спољни медијум за складиштење података;
23. CD-ROM (Compact disk - read only memory) користи се као медијум за складиштење података;
24. DVD је оптички диск високог капацитета који се користи за складиштење података.

## II. Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Вишег суда у Нишу, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

**Risk management** треба да открије, контролише и умањи утицај опасности.

**Анализа ризика (Risk Analysis)** је процес којим организација одређује вредност свих заштићених средстава, процењује вероватноћу да ће неко средство бити угрожено и упоређује могуће трошкове угрожавања тог средства са трошковима који су потребни да се то средство заштити.

**Ублажавање ризика (Risk Mitigation)** подразумева да организација предузме конкретне мере против ризика.

Ублажавање ризика има 2 функције:

1. Примена системске контроле која спречава појаву ризика-претње

2. Развој средстава за повраћај информација

Стратегије за ублажавање ризика:

1. Прихватање ризика-наставак пословања без контроле и прихватање штете која се појави

2. Ограничавање ризика-спровођењем контроле која смањује дејство претње

3. Пренос ризика-процес у коме организација користи нека средства да би надокнадила евентуалне губитке (нпр. полиса осигурања)

**Евалуација контроле** подразумева утврђивање недостатака безбедности и утврђивање трошкова имплементације адекватних мера контроле. Контроле безбедности су пројектоване тако да заштите све компоненте ИКТ система.

Врсте контроле:

1. Физичка контрола
2. Контрола приступа
3. Контрола комуникација
4. Контрола апликација

**1. Организациона структура, са утврђеним пословима и одговорностима запослених, којима се остварује управљање информационом безбедношћу у Вишем суду у Нишу**

Члан 6.

Сваки запослени-корисник ресурса ИКТ система је одговоран 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 надлежан је систем администратор Вишег суда у Нишу.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава и имовине за надзор над пословним процесима од значаја за информациону безбедност
- послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности
- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава односно информационих добара ИКТ система Вишег суда у Нишу као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе
- праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу
- обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима

**2. Безбедност рада на даљину и употреба мобилних уређаја**

Члан 7.

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

**3. Обезбеђење да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност**

Члан 8.

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места. Виши суд у Нишу 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.

Систем администратор је дужан да сваког корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса Вишег суда у Нишу.

Свако коришћење ИКТ ресурса Вишег суда у Нишу од стране запосленог-корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

**4. Заштита од ризика који настају при променама послова или престанка радног ангажовања запосленог-корисника ИКТ система**

Члан 9.

У случају промене послова, односно надлежности корисника-запосленог, администратор система ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

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

О престанку радног односа или радног ангажовања као и промени радног места систем администратор је дужан да се информише у персоналној служби суда ради укидања, односно измене приступних привилегија за тог 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. Идентификовање информационих добара и одређивање одговорности за њихову заштиту**

Члан 10.

Информациона добра су сви ресурси који садрже пословне информације Вишег суда у Нишу, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем и сл.

Евиденцију о информационим добрима води систем администратор у папирној или електронској форми.

Предмет заштите обухвата:

- хардверске и софтверске компоненте ИКТ система
- податке који се обрађују или чувају на компонентама ИКТ система
- корисничке налоге и друге податке о корисницима информатичких ресурса ИКТ система

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

Члан 11.

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. 53/2011).

**7. Заштита носача података**

Члан 12.

Подаци могу да се сниме (архивирају, запишу) на серверу на коме 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 (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених-корисника.

Носачи информација морају бити прописано обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта носача информација председник суда ће одредити одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на носачима, подаци морају бити трајно обрисани, ако то није могуће, такви носачи морају бити физички оштећени односно уништени.

**8. Ограничење приступа подацима и средствима за обраду података**

Члан 13.

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

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

Запослени-корисник може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, сем администратору за подешавање 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:

1. користи информатичке ресурсе искључиво у пословне сврхе;
2. прихвати да су сви подаци који се складиште, преносе или процесуирају у оквиру информатичких ресурса власништво Вишег суда у Нишу и да могу бити предмет надгледања и прегледања;
3. поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. безбедно чува своје лозинке, односно да их не одаје другим лицима;
5. мења лозинке сагласно утврђеним правилима;
6. пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу;
7. обезбеди сигурност података у складу са важећим прописима;
8. приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
9. не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
10. на радној станици не сме да складишти садржај који не служи у пословне сврхе;
11. израђује заштитне копије података у складу са прописаним процедурама;
12. користи интернет и електронску пошту у складу са прописаним процедурама;
13. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
14. прихвати да технике сигурности (анти вирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;
15. не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер;

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

Члан 14.

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 Нишу.

Кориснички налог се састоји од корисничког имена и лозинке на основу којих се врши аутентификација - провера идентитета 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.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог на пословима управљања људским ресурсима, односно надлежног руководиоца.

Сви запослени у Вишем суду имају приступ ИТ систему Вишег суда, али се зато морају придржавати следећих правила у вези свог корисничког налога како би се заштитила безбедност мреже, интегритет података као и система уопште:

- Сваки запослени у Вишем суду има своје индивидуално корисничко име, као и своју шифру
  - За приступ ИТ систему Вишег суда;
  - За АВП програм
  - За електронску пошту
  - За електронску базу судских одлука

- Сви кориснички налози имају следећа подешавања за шифре
  - Минимални број карактера је 6
  - Шифру чини комбинација алфабетских, нумеричких као и знакова интерпункције
  - Корисници су у обавези да промене своју шифру приликом првог пријављивања на мрежу од дана ступања на снагу Акта о безбедности информационих система Вишег суда.
  - Корисници би требали да на сваких 6 месеци мењају своје корисничке шифре.
  - Кориснички налози се закључавају после 3 неуспешна покушаја пријављивања на исти
- Корисничке шифре не би требало да могу лако да се погоде (Корисничка шифра не треба бити: лична имена и презимена, године, датум или место рођења, део корисничког налога, итд.)
- Корисници не би требали да користе опцију „Запамти шифру“ апликативних програма, као што је Internet Explorer
- Корисничке шифре не би требале бити записане, и сем корисника нико не би требао да је зна. Власник корисничког имена је одговоран за све акције извршене под тим корисничким именом док се не утврди супротно.
- Корисници не треба да дозволе коришћење њихових корисничких имена некој другој особи, било да та друга особа је такође запослена у Вишем суду или да је реч о неком трећем лицу.
- Ако их неко пита за њихов кориснички налог и шифру, корисници су у обавези да их упуте на одељење за информатичке службе Вишег суда, као и да сами пријаве такав захтев. Такође, ако

постоји сумња да је шифра њиховог корисничког налога „коришћења без њиховог знања“, корисници одмах то пријављују информатичкој служби Вишег суда.

- Захтев за нови налог рачунара или корисника, као и брисање постојећег мора бити формално ауторизовано од стране Управе суда, као и Одељења за информационо-комуникационе технологије (ИТ Одељење) Вишег суда.
- Управа суда **треба писмено обавештавати** одељење за информатику о промени запослених у суду, како би **списак запослених са корисничким именима био ажуран**. По пријему обавештења о промени запослених од Управе суда, ИТ одељење је у обавези да у што краћем року (препорука: у текућем радном дану) направи или избрише корисничко име.
- Захтев за приступ одређеном делу мреже или одређеној апликацији такође мора бити формално и у писаној форми одобрено од стране ИТ одељења Вишег суда. Ако Виши суд нема права тј. лиценцу за одређену тражену апликацију, ИТ одељења Вишег суда ће се консултовати са Председником Вишег суда, Сектором за ИТ технологије Министарства правде РС, као и рачуноводством суда о неопходности и могућностима одређеног захтева.

## 10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15.

Аутентификације корисника којима је одобрен приступ систему врши се путем јединственог корисничког имена и лозинке.

Корисници су дужни да корисничко име и лозинку држе у тајности и не откривају другим лицима укључујући и надређене особе.

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 податке.

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

Члан 16.

Приступ ресурсима ИКТ Вишег суда у Нишу не захтева посебу криптозаштиту.

**12. Физичка заштита објекта, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему**

Члан 17.

Виши суд у Нишу је дужан да предузме мера 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 ометања информација.

Простор у коме се налазе сервери, мрежна и комуникациона опрема ИКТ сустема, организује се као административна зона.

Простор мора да буде обезбеђен од компромитујућег електомагнетног зрачења(КЕМЗ), пожара и других елементарних непогода, у њему треба да буде одговарајућа температура(климатизовани простор) и забрањен приступ незапосленим лицима;

Да би приступили сервер сали Вишег суда, трећа лица морају добити оверено писмено одобрење службе за информатику Вишег суда.

Трећа лица којима је одобрен приступ сервер сали Вишег суда тамо могу приступити само уз присуство овлашћеног лица.

Сервер сала Вишег суда треба да буде опремљена видео надзором.

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

Члан 18.

Улаз у просторије у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система и запосленим-корисницима ИКТ система.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, уз присуство надлежног лица.

Приступ административној зони могу имати 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 Вишег суда мора бити опремљена детекторима дима и пожара, који треба да се подеси на аутоматски рад.

Опрема за детекцију и спречавање пожара мора бити тестирана бар једном годишње.

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

UPS генератор мора бити тестиран бар једном годишње.

Сервери и активна мрежна опрема (switch, modem, router, firewall) морају стално бити прикључени на уређаје за непрекидно напајање електричном енергијом - УПС.

У случају нестанка електричне енергије, у периоду дужем од капацитета УПС-а овлашћено 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 обаља 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 Нишу.

## 14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Запослени на пословима ИКТ система континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и у складу са 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 сучају да се на новој верзији софтвера који је уведен у оперативни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

## 15. Заштита података и средстава за обраду података од злонамерног софтвера

Члан 20.

ИКТ систем Вишег суда у Нишу представља део јединственог информационог система правосудних органа. У складу са тим, превентивне мере као и мере заштите података прописане на нивоу ИКТ система правосудних органа примењују се и у ИКТ систему Вишег суда у Нишу.

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

За успешну заштиту од злонамерног софтвера Виши суд у Нишу своју делатност обавља преко „Правосудне WAN" мреже која има ограничен приступ, такоде на сваком рачунару је инсталиран антивирусни програм који се свакодневно аутоматски ажурира.

Употреба преносивих медија – USB меморија од стране корисника није омогућена.

Уколико је неопходо коришћење преносивог медија, може се омогућити једнократно коришћење истог. Преносиви медији пре коришћења морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, врши се чишћење медија од вируса, уз сагласност доносиоца медија. Ризик од евентуалног губитка података приликом чишћења медија антивирусним софтвером, сноси доносилац медија.

Приликом коришћења интернета треба избегавати сумњиве WEB странице, с обзиром да то може проузроковати проблеме – неприметно инсталирање шпијунских програма.

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 на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимања (download) података велике „тежине" који проузрокују „загушење" на мрежи;
- преузимање (download) софтвера и материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видео стриминг и сл.);
- недозвољен приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета

Запосленим-корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарашавају безбедност мреже може се одузети право приступа.

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

- службене налоге за електронску пошту користити искључиво за службену комуникацију пријављиавање на сервисе из оквира пословног окружења(не користити их за личну комуникацију, прослеђивање ланчаних порука, за пријаве на сервисе електронског банкарства, комуналних услуга и друге приватне потребе)
- електронска пошта са прилозима не сме се отварати ако долази са сумљивих и непознатих адреса, већ се мора избрисати
- не попуњавати (не слати) податке као што су нпр. корисничко име, лозинка, бр. телефона, алтернативна адреса електронске поште и сл. јер је у питању покушај злоупотребе
- не прихватати опције за покретање неког програма/апликације уколико се при отварању документа из прилога појави порука типа „ок/сагласан“

**16. Заштита од губитка података**

Члан 21.

Виши суд у Нишу врши израду резервних копија које обухватају системске информације и податке који су неопходни за опоравак система у случају наступања последица изазваних ванредним околностима.

Заштита од губитка података у Вишем суду у Нишу обезбеђује се креирањем резервних копија на backup серверу.

Одељење за информационе технологије мора да прави редовне дневне, недељне и месечне резервне копије система и података.

За резервне копије система и података ИТ одељење ће користити сервер резервних копија који ће се налазити одвојено од сервер сале у којој се налазе сви сервери Вишег суда.

ИТ одељење ће правити резервне копије система свих сервера у Вишем суду, података из АВП програма као и саме апликације, као и свих осталих релевантних података корисника на серверу.

Корисници увек треба да чувају пословне податке и датотеке и **на мрежи, а не само на локалном рачунару.** Овај поступак осигурава да се редовно праве резервне копије тих података и да је могућ њихов опоравак у случају краха рачунара или ИТ система. ИТ служба Вишег **суда неће имати копију података са локалних рачунара осим ако другачије није договорено. Корисници су дужни да редовно воде рачуна о својим подацима и биће лично одговорни за њихову безбедност. Сваки губитак података, преснивање преко документа и слично, не одговара ИТ служба Вишег суда.**

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

Члан 22.

О активностима администратора и запослених-корисника воде се дневници активности (activity log, history, security log, transaction log и др.).

## 18. Обезбеђење интегритета софтвера и оперативних система

Члан 23.

Виши суд у Нишу спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за контролу промена и инсталацију софтвера.

Смернице за контролу промена и инсталацију софтвера

- Ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљени администратори, по добијању одговарајућег овлашћења од руководиоца;
- Оперативни системи треба да садрже само одобрене извршне кодове, а не и развојне кодове или компилаторе;
- Апликације и оперативни системски софтвер треба имплементирати тек после обимног и успешно спроведеног испитивања, које обухвата испитивање применљивости, безбедности, утицаја на друге системе и погодности за коришћење, а треба их спроводити на засебним системима, односно тестним окружењима;
- Треба осигурати да су све одговарајуће библиотеке изворних програма ажуриране;
- Пре имплементације било каквих промена, треба успоставити стратегију повратка на претходно стање;
- Као меру предострожности за неочекиване ситуације треба сачувати претходне верзије апликативног софтвера;

Инсталацију и подешавање софтвера може да врши само систем администратор Вишег суда у Нишу.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера.

## 19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, систем администратор је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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

## 20. Обезбеђење да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Члан 25.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених. Предмет и подручје испитивања за проверу су унапред договорени и строго

контролисани. Уколико то није могуће у радно време, онда се ревизија врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност председника суда.

**21. Заштита података у комуникационим мрежама укључујући уређаје и водове**

Члан 26.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, router, firewall) мора бити обезбеђена и лоцирана на прописаним местима, доступна систем администратору који је дужан да врши контролу целокупне мрежне опреме и благовремено преузима мере у циљу отклањања евентуалних неправилности.

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

Члан 27.

Заштита података који се преносе комуникационим средствима унутар Вишег суда у Нишу, између Вишег суда у Нишу и лица ван Вишег суда у Нишу обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума као и применом адекватних контрола.

Правила коришћења електронске поште, интернета и информационих ресурса прописана су на нивоу ИКТ система правосудних органа и чланом 20. овог Правилника.

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

Члан 28.

ИКТ систем Вишег суда у Нишу представља део јединственог информационог система правосудних органа. У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, потребно је обезбедити информациону безбедност у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења.

Систем администратор суда је задужен за технички надзор над реализацијом од стране извођача, односно испоручиоца.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система, администратор система води документацију која садржи описе свих урађених процедура.

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

Члан 29.

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.

Уколико је за тестирање неопходно користити оперативне податке, примењују се следеће смернице:

- За свако копирање оперативних података у тестно окружење се издаје посебно овлашћење;
- Приликом тестирања апликативних система примењују се процедуре за контролу приступа које се примењују и на оперативним системима;
- Оперативне информације се одмах по завршетку испитивања бришу из тестног окружења.

За потребе тестирања ИКТ система односно делова система систем администратор суда може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

## 25. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 30.

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

Пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са Вишем судом у Нишу.

Виши суд у Нишу успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга:

- Идентификовање и документовање врсте пружаоца услуга којима ће Виши суд у Нишу дозволити да приступ информацијама;
- Стандардизовани процес за управљање односима између пружаоца услуга;
- Дефинисање врста информација које ће различитим типовима пружаоца услуга бити дозвољено ради приступања, праћења и контроле приступа;
- Минимални захтеви за безбедност информација за сваку врсту информација и врсту приступа;
- Процеси и процедуре за праћење придржавања утврђених захтева за безбедност за сваку врсту добављача и врсту приступа;
- Контроле за осигурање интегритета информација или обраде информација коју обезбеђује било која страна;
- Поступање са инцидентима и непредвиђеним ситуацијама које су у вези са приступом пружаоца услуга, укључујући одговорности и организације и пружаоца услуга;
- Управљање неопходним променама информација, опреме за обраду информација и свега осталог што треба да се премешта и осигурање да се безбедност информација одржава током прелазног периода

Пре отпочињања преговора, потенцијални пружалац услуга у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, која садржи обавезу за пружаоца услуга да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране Виши суда у Нишу, а за потребе извршења предмета преговора.

Пример: „Сви подаци и информације садржани у овом Уговору о пружању услуга се сматрају поверљивим пословним подацима и не смеју бити саопштени или на други начин учињени доступним трећим лицима. Нарочито се сматрају поверљивим сви пословни подаци и информације које једна страна учини доступним другој уговорној страни ради извршења обавеза из овог уговора, уколико ти подаци нису јавно доступни нити су били претходно познати другој страни.

Уговорне стране се нарочито обавезују да поступају обазриво са подацима о личности до којих могу доћи у поступку извршења услуга за оператора ИКТ система, као и да те податке чувају и поступају у свему у складу са прописима који уређују заштиту података о личности.

У случају повреде ове обавезе уговорна страна чији су подаци коришћени има право раскида уговора и право да захтева накнаду штете услед неовлашћеног коришћења података и информација друге стране.

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

Члан 31.

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

Систем администратор редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

1. Надгледање и преиспитивање услуга се може вршити преко трећег лица;
2. Неопходно је да се поштују сви услови из споразума у вези са безбедношћу информација, као и да се спрече сви инциденти и проблеми нарушавања безбедности, те омогући управљање на одговарајући начин;
3. Врши се оцена квалитета извршења и саобразности уговорене услуге;
4. Пружалац услуге има уговорну обавезу да организује и припреми периодичне састанаке који ће обезбедити редовно извештавање Вишег суда у Нишу и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;
5. Систем администратор одржава потпуну контролу над спровођењем услуга и осигурава увид у све осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа страна приступа, које процесуира или којима управља;
6. Систем администратор одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања;
7. Преиспитује трагове провере и записа о догађајима у вези са безбедношћу код пружаоца услуга, односно оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене; утврдити поступак извештавања, праћења и поступања у складу са захтевима Вишег суда у Нишу у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета пружаоца услуга.

Приликом надзора над извршењем квалитета и саобразности уговорене услуге проверава се да ли пружалац услуге задовољава све критеријуме који су били од пресудног значаја приликом избора, укључујући обим и квалитет услуге, као и да се у току поступка извршења услуге може утицати на побољшање квалитета услуге или начина и обима извршења, у складу са утврђеним стварним потребама суда.

У поступку објективне евалуације квалитета и обима пружене услуге у односу на уговорену, потребно је прикупити све релевантне чињенице, податке и документацију у вези са извршењем услуге, као и прикупити податке од непосредних, крајњих, корисника у вези са предметом услуге. Евалуација се може извршити слањем упитника, разговором са изабраним појединцима или на основу анонимног анкетирања путем електронске поште.

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 Виши суд у Нишу ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

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

Члан 32.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести систем администратора.

По пријему пријаве систем администратор је дужан да о томе обавести председника суда и преузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Урдебом о поступку обавештавања о инцидентима у ИКТ системима од посебног значаја, („Сл. Гласник РС“ бр. 11/2020), систем администратор је дужан да поред председника суда обавести и надлежни орган дефинисан овом уредбом.

Систем администратор води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које против одговорног лица могу да се воде дисциплински, прекршајни или кривични поступци.

**28. Мере које обезбеђују континуитет обављања посла у ванредним ситуацијама**

Члан 33.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде суда систем администратор је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Делови ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди председник суда. Складиштење делова ИКТ система који нису неопходни, врши се тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води.

**III Измена Правилника о безбедности**

Члан 34.

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 безбедност, систем администратор је дужан да обавести председника суда, како би он могао да приступи измени овог правилника, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу ресурса ИКТ система.

## IV Провера ИКТ система

Члан 35.

Проверу ИКТ система врши систем администратор Вишег суда у Нишу.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на које се врши упућивање, са прописаним условима односно проверава се да ли су правилником адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему
2) провереава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама интервјуа, симулације, посматрања, увида у предвиђене евиденције и другу документацију,
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 познатих безбедносних слабости у сличним окружењима

О извршеној провери сачињава се извештај, који се доставља председнику суда.

## V Садржај извештаја о провери ИКТ система

Члан 36.

Извештај о провери ИКТ система садржи:

- назив оператора ИКТ система који се проверава
- време провере
- подаци о лицима која су вршила проверу
- извештај о спроведеним радњама
- закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима
- закључке по питању адекватне примене предвиђених мера заштите у оперативном раду
- оцена укупног нивоа информационе безбедности
- предлог евентуалних корективних мера
- потпис одговорног лица које је спровело проверу ИКТ система

**VI Прелазне и завршне одредбе**

Члан 37.

Овај Правилник ступа на снагу наредног дана од дана објављивања на огласној табли и интернет страници Вишег суда у Нишу.

У Нишу, 14.02.2022. године

Информатичко Одељење
Вишег Суда у Нишу
Шеф ИТ одељења
Драган Миладиновић

Председник Вишег суда у Нишу
Драгана Живадиновић