РЕПУБЛИКА СРБИЈА
НАРОДНА СКУПШТИНА
03 Број: 02 - 1936/17
10. јул 2017. године
Београд

На основу члана 8. Закона о информационој безбедности ("Службени гласник РС", број 6/16), члана 69. став 1. Закона о Народној скупштини („Службени гласник РС“, бр. 9/10 и 108/13-др. закон), члана 2. Уредбе о ближем садржају акта о безбедности информационо - комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо - комуникационих система од посебног значаја ("Службени гласник РС", број 94/16 од 24.11.2016. године), тач 4. и 6. Одлуке о организацији и раду Службе Народне скупштине („Службени гласник РС“, број 49/11), генерални секретар Народне скупштине доноси

# ПРАВИЛНИК
# О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНИХ СИСТЕМА НАРОДНЕ СКУПШТИНЕ РЕПУБЛИКЕ СРБИЈЕ

## Предмет

Члан 1.

Овим правилником ближе се дефинишу мере заштите информационо-комуникационих система у Народној скупштини Републике Србије (у даљем тексту: НСРС), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса у НСРС.

## Циљеви

Члан 2.

Циљеви доношења овог правилника су:

1) допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;

2) минимизација безбедносних инцидената;

3) допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистентне контроле свих компонената информационо - комуникационог система (у даљем тексту: ИКТ систем).

## Обавезност

Члан 3.

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

Непоштовање овог правилника повлачи дисциплинску одговорност корисника информатичких ресурса.

За праћење примене овог правилника надлежно је Одељење за електронику, телекомуникације и информатику.

## Појмови

Члан 4.

Поједини изрази употребљени у овом правилнику имају следеће значење:

**1)** интегритет је немогућност неовлашћене измене информација;

**2)** расположивост је доступност информација корисницима информатичких ресурса у обиму корисничког овлашћења;

**3)** тајност је обезбеђивање доступности информација само овлашћеним корисницима информатичких ресурса, као и немогућност приступа информацијама лицима која немају таква овлашћења;

**4)** администраторско овлашћење је право креирања, доделе, блокирања и укидања корисничких налога за приступ информатичким ресурсима;

**5)** кориснички налог јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно овлашћења корисника);

**6)** администраторски налог јесте јединствен налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога.

## Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности НСРС, 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.

## Информатички ресурси НСРС

Члан 6.

Информатички ресурси НСРС су сви ресурси који садрже пословне информације НСРС у електронском облику или служе за приступ корисника ИКТ систему укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и слично.

## Предмет заштите

Члан 7.

Предмет заштите обухвата:

1) хардверске и софтверске компоненте информатичких ресурса;

2) податке који се обрађују или чувају на информатичким ресурсима;

3) корисничке налоге и друге податке о корисницима информатичких ресурса у НСРС;

## Корисник информатичких ресурса

Члан 8.

Корисник информатичких ресурса јесте постављено лице, запослено лице на неодређено или одређено време, лице ангажовано по основу уговора, консултант или друго радно ангажовано лице коме је одобрен приступ неком информатичком ресурсу НСРС.

Корисник информатичких ресурса одговоран је за правилну употребу, тачност и сигурност података приликом коришћења информатичких ресурса НСРС, односно лично је одговоран за остваривање својстава података у ИКТ систему НСРС.

Корисник информатичких ресурса нема имовинска права над информатичким ресурсима НСРС.

## Дужности корисника информатичких ресурса

Члан 9.

Корисник не сме спроводити активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система НСРС.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне сврхе, а НСРС задржава право да информатичке ресурсе повуче у било ком тренутку и у потпуности задржи све податке без обавезе да их накнадно преда кориснику.

Корисник непреносиве радне станице је дужан да пословне податке смешта на самој радној станици или на одређене мрежне дискове на серверу НСРС.

Корисник преносиве радне станице има право да привремено смешта пословне податке на локални диск преносиве радне станице, као и обавезу да уради копију битних докумената са локалног диска на мрежни диск сервера НСРС.

Запослено, односно ангажовано лице у Одељењу за електронику, телекомуникације и информатику са администраторским овлашћењима (у даљем тексту: администратор), као и лица која су задужена за израду резервних копија, дужни су да дневно израђују резервне копије података са мрежних дискова НСРС.

Корисник информатичких ресурса дужан је да поштује следећа правила безбедног и примереног коришћења информатичких ресурса и то:

**1)** да користи информатичке ресурсе искључиво у пословне сврхе;

**2)** прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво НСРС 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)** пре сваког удаљавања од радне станице одјави се са система (*"log out"*);

**6)** користи *DVDRW*, *CDRW* и *USB* екстерне меморије на радној станици само уз одобрење Одељења за електронику, телекомуникације и информатику, а на основу образложеног предлога непосредног руководиоца;

**7)** захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца и Начелника Одељења за електронику, телекомуникације и информатику;

**8)** обезбеди сигурност података у складу са важећим прописима;

**9)** приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;

**10)** не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;

**11)** не сме да на радној станици складишти садржај који не служи у пословне сврхе;

**12)** израђује заштитне копије (*backup*) података у складу са прописаним процедурама;

**13)** користи ИНТЕРНЕТ и *E-MAIL* сервис у НСРС у складу са прописаним процедурама;

**14)** прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, *upgrade firmware*, покретање антивирусног програма и сл.) обављају у утврђено време;

**15)** прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;

**16)** 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;

**17)** не сме да инсталира, модификује, искључује из рада или брише, заштитни, системски или апликативни софтвер;

**18)** да се уздржи од активности којима се изазива неоправдано оптерећење информатичких ресурса НСРС, као и повећано ангажовање особља на одржавању тих ресурса;

**19)** не сме неовлашћено да објављује или преноси личне податке до којих је дошао коришћењем информатичких ресурса НСРС, као што су лозинке, бројеви платних картица, медицински подаци, приватни телефонски бројеви итд. и да тиме повреди приватност појединаца;

**20)** да се уздржи од неуобичајено и неоправдано великог коришћења информатичких ресурса НСРС, а посебно у приватне сврхе.

**Безбедносни профил корисника информатичких ресурса**

Члан 10.

У зависности од описа задатака и послова радног места на које је распоређен, корисник информатичких ресурса, на предлог непосредног руководиоца, стиче одређена права приступа ИКТ систему НСРС.

Администраторска овлашћења могу добити само лица која су задужена за одржавање информатичких ресурса у НСРС, уз претходну сагласност Начелника Одељења за електронику, телекомуникације и информатику.

**Креирање лозинке**

Члан 11.

Лозинка мора да садржи минимум осам карактера комбинованих од малих и великих слова и цифара.

Корисник лозинку мора променити у року од 3 месеца о чему ће бити благовремено обавештен од стране система

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

Корисник користи једну лозинку која служи за аутентификовање на рачунару, е-парламенту, *mail* налогу и конектовање на бежичну рачунарску мрежу.

Ако корисник информатичких ресурса посумња да је друго лице открило његову лозинку, дужан је да се писмено обрати администратору који ће лозинку променити.

Иста лозинка се не сме понављати у периоду од годину дана.

**Употреба корисничког налога**

Члан 12.

Кориснички налог може употребљавати само корисник информатичких ресурса коме је исти издат.

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору у случају подешавања радне станице.

Корисник информатичких ресурса је непосредно одговоран за активности које су реализоване на основу његовог корисничког налога.

Кориснички налози са администраторским овлашћењима користе се само за потребе неопходних интервенција којима се обезбеђује несметан рад информатичких ресурса (у даљем тексту: информатичке интервенције).

**Употреба администраторског налога**

Члан 13.

Администраторски налози свих пословних апликација, сервера база података и системских апликација за управљање мрежном опремом и уређајима за складиштење података чувају се у затвореним, непровидним ковертама са отиском службеног печата, у сефу НСРС, којој има приступа само лице које је за исту задужено.

Право коришћења администраторског налога имају само администратори за потребе информатичких интервенција.

**Поступци у случајевима сигурносних инцидената**

Члан 14.

Корисник информатичких ресурса дужан је да, без одлагања, пријави непосредном руководиоцу свако уочавање или сумњу о наступању инцидента којим се угрожава сигурност ИКТ система.

Информацију о инциденту руководилац из става 1. овог члана дужан је да одмах проследи администратору, као и Одељењу за електронику, телекомуникације и информатику

По пријави инцидента мора се поступати адекватно и ефикасно, а по хитном поступку у случајевима:

1) нарушавања поверљивости информација,

2) откривања вируса или грешака у функционисању апликација,

3) вишеструких покушаја неауторизованог приступа,

4) системских падова и престанка рада сервиса.

Одељење за електронику, телекомуникације и информатику је дужно да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести надлежни орган, у складу са законом којим се уређује информациона безбедност.

**Заштита од малициозног софтвера**

Члан 15.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена:

1) лиценцираног софтвера, односно забрана коришћења неауторизованог софтвера;

2) правила за заштиту од ризика приликом преузимања фајлова из екстерних извора (података, апликација и сл.)

Приликом преузимања фајлова из става 1. тачка 2) овог члана 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.

**Сигурност електронске поште**

Члан 16.

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

1) електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;

2) забрањено је коришћење електронске поште у приватне сврхе; не смеју се користити приватни налози електронске поште у пословне сврхе.

**Поступање са преносивим медијима**

Члан 17.

Преносиви медији који садрже податке морају да буду прописно обележени и пописани.

У случају брисања података који се налазе на преносивим медијима, потребно је обезбедити њихово неповратно брисање.

Преносиви медији из става 1. овог члана, пре стављања ван употребе, морају бити физички уништени.

## Физичка сигурност информатичких ресурса

Члан 18.

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови:

1) сервери, уређаји за складиштење (*storage*) и комуникационо чвориште у просторијама НСРС морају бити смештени у посебној просторији (север соби), која испуњава стандарде противпожарне заштите и поседује резервно напајање електричном струјом и адекватну климатизацију и којој је забрањен приступ незапосленим лицима;

2) приступ сервер соби, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење Начелника Одељења за електронику, телекомуникације и информатику;

3) радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;

4) просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;

5) штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;

6) медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

## Приступ ИКТ систему НСРС

Члан 19.

Приступ свим компонентама ИКТ система мора бити аутентификован.

Администратор, на основу прецизног писаног захтева непосредног руководиоца, додељује кориснику информатичког ресурса корисничко име, лозинку и привилегије, као и налог за електронску пошту и Е-парламент апликацију.

Кориснику информатичких ресурса додељују се само привилегије које су неопходне за реализацију његових радних обавеза.

У случају престанка радног односа, или радног ангажовања у НСРС, кориснику информатичког ресурса укида се право приступа ИКТ систему.

У случају одсуства са посла дуже од месец дана, кориснику информатичког ресурса се привремено укида право приступа ИКТ систему, до повратка на посао.

О престанку радног односа или радног ангажовања, одсуству са посла дуже од месец дана, као и о промени радног места корисника информатичких ресурса, непосредни

руководилац је дужан да обавести Одељење за електронику, телекомуникације и информатику ради укидања, односно измена приступних привилегија тог корисника.

Корисник информатичких ресурса, након престанка радног ангажовања у НСРС, не сме да открива поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система.

Корисник информатичких ресурса може имати удаљени (*remote*) приступ ИКТ систему. Удаљени приступ може имати искључиво уз писано одобрење Генералног секретара Народне скупштине Републике Србије.

Трећем лицу се могу одобрити права приступа ИКТ систему уз претходно склапање одговарајућег уговора, којим се прецизно дефинишу услови и обим права приступа, укључујући и све релевантне безбедносне захтеве.

Изузетно од става 8. овог члана, у случају неопходних и хитних послова, могу се одобрити права приступа трећем лицу по усменом налогу Генералног секретара Народне скупштине Републике Србије, односно овлашћеног лица, о чему ће се накнадно, по завршетку посла, сачинити записник о оствареном приступу.

Ако се установи повреда уговорне обавезе или прекорачење овлашћења по основу уговора, одобрени приступ се одмах укида.

**Инсталација и одржавање софтвера**

Члан 20.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужени су администратори, који су дужни да поступају у складу са прописаним процедурама и упутствима.

Одељење за електронику, телекомуникације и информатику обезбеђује запосленом, односно ангажованом лицу, коришћење радне станице, (десктоп или лаптоп) са инсталираним, правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачки програми (драјвери), пословно и развојно окружење, софтвер за вирусну заштиту, разне помоћне апликације), који је типски за све радне станице и који представља минимум потребан за обављање стандардних послова.

Администратор врши оцену конзистентности траженог софтвера са постојећим инсталираним софтвером на предметној радној станици и уколико оцени да тражени софтвер неће угрозити или ометати рад, инсталираће захтевани софтвер, искључиво лиценцирану или бесплатну верзију.

Основна подешавања из става 2. овог члана су:

1) додељивање имена, TCP/IP адресе радној станици и њено придруживање домену;

2) подешавање *mail* клијента;

3) подешавање *web* претраживача;

4) подешавање е-парламента;

5) инсталација лиценцираног антивирус софтвера одобреног од стране Одељења за електронику, телекомуникације и информатику;

6) инсталација званичног апликативног софтвера који одређене унутрашње јединице НСРС користе у свом раду.

У случају да је кориснику потребно да се изврши инсталација одређеног специфичног софтвера на радној станици, непосредни руководилац подноси захтев електронским путем Одељење за електронику, телекомуникације и информатику.

Корисник информатичког ресурса дужан је да сваки проблем у функционисању оперативног система, *mail* клијента, *web* претраживача, пословног софтвера и апликативног софтвера, пријави непосредном руководиоцу који ову информацију прослеђује електронским путем Одељењу за електронику, телекомуникације и информатику.

Проблем у функционисању антивирусног софтвера мора се пријавити без одлагања.

Администратор је дужан да проблеме из става 6. и 7. овог члана отклони у најкраћем могућем року на локацији корисника, даљинском конекцијом ка радној станици или доношењем радне станице у Одељење за електронику, телекомуникације и информатику.

Члан 21.

Овај правилник ступа на снагу даном доношења.

ГЕНЕРАЛНИ СЕКРЕТАР

Светислава Булајић