На основу члана 8. Закона о информационој безбедности („Сл. гласник РС“ бр. 6/2016, 94/2017 и 77/2019), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. гласник РС“, бр. 94/2016), члана 31. Статута ЈКП Путеви Рашка, а на предлог директора у складу са тачком 11члана 35., Статута ЈКП Путеви Рашка, Надзорни одбор ЈКП Путеви Рашка, на седници одржаној дана 27.01.2021. године доноси

# ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА У ЈКП ПУТЕВИ РАШКА

## *I Опште одредбе*

### Члан 1.

Овим правилником се утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система ЈКП Путеви Рашка (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система који користи ЈКП Путеви Рашка.

Мере прописане овим правилником се односе на све секторе ЈКП Путеви Рашка, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе ЈКП Путеви Рашка.

Непоштовање одредби овог правилника повлачи законску одговорност запосленог-корисника информатичких ресурса ЈКП Путеви Рашка.

### Члан 2.

Поједини термини у смислу овог правилника имају следеће значење:

1) оператор је ЈКП Путеви Рашка које, у оквиру обављања своје делатности, односно за обављање послова из своје надлежности, користи ИКТ систем;

2) ИКТ систем је технолошко-организациона целина која обухвата:

- електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
- 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;
- податке који се похрањују, обрађују, претражују или преносе помоћу средстава из претходних подтачака ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКТ системом;

4) 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 и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

5) тајност је својство које значи да податак није доступан неовлашћеним лицима;

6) интегритет значи очуваност изворног садржаја и комплетности податка;

7) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

8) 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;

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

10) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

11)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;

12) инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

13) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

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

15) ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

16) компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

17) криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

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

19) криптографски производ је софтвер или уређај путем кога се врши криптозаштита;

20) криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

21) безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

22) информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

23) VPN (Virtual Private Network) је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;

24) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;

25) Backup је резервна копија података;

26) Download је трансфер података са централног рачунара или web презентације на локални рачунар;

27) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;

28) Freeware је бесплатан софтвер;

29) Opensource софтвер је софтвер отвореног кода;

30) Firewall је „заштитни зид" односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

31) USB или флеш меморија је спољашњи медијум за складиштење података;

32) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;

33) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

34) надлежни субјект ИКТ система-лице одређено од стране директора предузећа.

## *II. Мере заштите*

**Члан 4.**

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

**Члан 5.**

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 ЈКП Путеви Рашка надлежно је лице које одреди директор предузећа, ако није другачије одређено.

**Члан 6.**

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност
- послови управљање 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 ЈКП Путеви Рашка, 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.

У случају инцидента руководилац сектора обавештава директора предузећа који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

**Одговорности корисника за заштиту сопствених средстава за аутентификацију**

**Члан 9.**

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира по матрици име. презиме, латиничним писмом без употребе слова ђ, ж, љ, њ, ћ, ч, џ, ш. Уместо ових слова користе се слова из следеће табеле:

| Ћирилична слова | Латинична слова |
|---|---|
| ђ | dj |
| ж | z |
| љ | lj |
| њ | nj |
| ћ, ч, ш | c |
| џ | dz |

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

Лозинка не сме да садржи препознатљиве податке корисника ИКТ система.

Ако корисник ИКТ система посумња да је друго лице открило његову лозинку дужан је да о томе одмах обавести надлежни субјект ИКТ система.

Корисник ИКТ система дужан је да мења лозинку у складу са потребама.

Неовлашћено уступање корисничког налога другом лицу подлеже дисциплинској одговорности.

За послове извршене под одређеним корисничким именом и лозинком одговоран је корисник ИКТ система којем су додељени.

## *III Предмет, мере и субјекти заштите ИКТ система*

### Предмет заштите ИКТ система

**Члан 10.**

Предмет заштите ИКТ система су:

- хардверске и софтверске компоненте ИКТ система,
- подаци који се обрађују или чувају на компонентама ИКТ система и
- кориснички налози и други подаци о корисницима иноформатичких ресурса ИКТ система.

### Мере и субјекти заштите ИКТ система

**Члан 11.**

Мере прописане овим правилником се односе на све секторе Оператора, на све кориснике ИКТ система Оператора, као и на трећа лица која користе информатичке ресурсе Оператора.

**Члан 12.**

Мерама заштите ИКТ система Оператора обезбеђује се превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Ради заштите тајности, аутентичности и интегритета података, Оператор може да размотри коришћење одговарајућих мера криптозаштите.

**Члан 13.**

Послове из области безбедности ИКТ система Оператора обавља надлежни субјект ИКТ система.

### Обавезе корисника

**Члан 14.**

Корисник ИКТ система је дужан да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система:

1) да користи информатичке ресурсе искључиво у пословне сврхе;
2) да прихвати да су сви подаци који се складиште, преносе или обрађују у оквиру информатичких ресурса власништво Оператора и да могу бити предмет надгледања и прегледања;
3) да поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4) да безбедно чува своје лозинке у односу на друга лица;
5) да мења лозинке сагласно утврђеним правилима;
6) да се, пре сваког удаљавања од радне станице, одјави са система, односно закључа радну станицу;

7) да користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење надлежног субјекта ИКТ система;

8) да захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране надлежног руководиоца;

9) да обезбеди сигурност података у складу са важећим прописима;

10) да приступа информатичким ресурсима само на основу изричито додељених корисничких права од стране надлежног субјекта ИКТ система;

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

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

13) да израђује заштитне копије (backup) података у складу са прописаним процедурама;

14) да користи Интернет, Интранет и имејл сервис Оператора у складу са прописаним процедурама;

15) да прихвати да се одређене врсте информатичких интервенција обављају у утврђено време;

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

17) да прихвати инсталацију техника и програма у циљу сигурности ИКТ система;

18) да не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

## *IV Појединачне мере заштите*

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

**Члан 16.**

Простор у коме се налазе рачунари за вођење база података и централни рачунар (сервер), мрежна или комуникациона опрема ИКТ система, организује са као административна зона.

**Члан 17.**

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само запосленима у надлежном субјекту ИКТ система.

Осим лица из става 1. овог члана, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу директора предузећа.

Сервери и активна мрежна опрема (switch, modem, router, firewal), морају стално бити прикључени на уређаје за непрекидно напајање - UPS.

У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, овлашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.

У случају изношења опреме из просторије из става 1. овог члана ради селидбе или сервисирања, неопходно је одобрење директора предузећа који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења директора предузећа, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Уговором са сервисером обавезно се дефинише обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Оператера.

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

**Члан 18.**

Нерегистровани корисници путем мобилних уређаја могу приступити следећим ресурсима ИКТ система Оператора: Интернету, e-mail сервису и web site-у.

Корисници ИКТ система, могу путем мобилних уређаја или рачунара, који су у власништву Оператора и који су подешени од стране надлежног субјекта ИКТ система, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности као што су електронска пошта, поједине апликације везане за обављање посла и друго.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Кориснику ИКТ система је забрањена самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја неовлашћеним лицима.

**Члан 19.**

Приступ ресурсима ИКТ система са приватног уређаја није дозвољен, осим ако је уређај у власништву Оператора оштећен и није обезбеђена замена.

Сагласност на коришћење приватног уређаја у случају из става 1. овог члана даје директор.

Евиденцију приватних уређаја са којих ће бити омогућен приступ води надлежни субјект ИКТ система.

**Члан 20.**

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране надлежног субјекта ИКТ система.

Приватни уређаји са којих се може приступати ресурсима ИКТ система могу се користити само за обављање послова у надлежности корисника ИКТ система и то само у периоду када није могуће користити уређај у власништву Оператора.

Надлежни субјект ИКТ система је дужан да, пре предаје уређаја овлашћеном сервису, уради backup података који се налазе у мобилном уређају, а потом их обрише из уређаја, а да по извршеном сервисирању врати податке у мобилни уређај.

**Заштита носача података**

**Члан 21.**

Подаци који се налазе у ИКТ систему представљају тајни податак који је, у складу са прописима о тајности података, одређен или означен одређеним степеном тајности.

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. гласник РС“, бр. 53/2011).

**Члан 22.**

Надлежни субјект ИКТ система ће успоставити организацију приступа подацима, посебно онима који буду означени тајним у складу са Законом о тајности података, тако да документи са ознаком тајности могу да се сниме, односно архивирају или запишу на фајл серверу у фолдеру над којим ће право приступа имати само корисници ИКТ сервиса који на то буду имали право.

Документи са ознаком тајности може да сними на друге носаче (екстерни HDD, USB, CD, DVD), само директор предузећа или запослени којег директор предузећа овласти писаним путем.

Евиденцију носача на којима су снимљени подаци са ознаком тајности, води надлежни субјект ИКТ система.

Носачи на којима се налазе документи са ознаком тајности морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

Приликом брисања података за ознаком тајности са носача на којима су се налазили, подаци морају бити неповратно обрисани, а ако то није могуће, такви носачи морају бити физички оштећени, односно уништени.

**Заштита података и средстава за обраду података од злонамерног софтвера**

**Члан 24.**

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, email-ом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару се инсталира антивирусни програм.

**Заштита при коришћењу интернета**

**Члан 25.**

У циљу заштите, односно упада у ИКТ систем Оператора са интернета, надлежни субјект ИКТ система је дужан да одржава систем за спречавање упада.

Руководиоци сектора Оператора одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Надлежни субјект ИКТ система може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система којима је одобрено коришћење интернета дужни су да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се корисник прикључује на интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши надлежни субјект ИКТ система.

Приликом коришћења интернета корисник ИКТ система коме је одобрено коришћење интернета дужан је избегавати сумњиве WEB странице, у циљу спречавања инсталирања програма који могу нанети штету ИКТ систему.

У случају да корисник примети необично понашање рачунара, ту појаву је дужан да без одлагања пријави надлежном субјекту ИКТ система.

**Члан 26.**

Кориснику ИКТ система коме је дозвољено коришћење интернета, забрањено је гледање филмова и играње игрица на рачунарима и претраживање WEB страница које садрже порнографски и остали недоличан садржај, као и самовољно преузимање истих са интернета.

**Члан 27.**

Недозвољена употреба интернета обухвата и:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратски“ или других софтверских производа који нису лиценцирани на одговарајући начин;
- 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 друга врста недозвољених софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено одлуком надлежног органа Оператора;
- преузимање података у количини која проузрокује велико оптерећење на мрежи;
- преузимање материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом;
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

**Заштита од злоупотребе безбедносних слабости ИКТ система**

**Члан 28.**

Надлежни субјект ИКТ система периодично врши анализу активности у циљу идентификације потенцијалних слабости ИКТ система.

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

**Заштита опреме ИКТ система**

**Члан 29.**

Комуникациони каблови и каблови за напајање морају бити постављени у зид или каналнице, тако да се онемогући неовлашћен приступ, односно да се изврши изолација.

Мрежна опрема (switch, router, firewall), морају се налазити у rack орману (метални орман), закључани.

**Безбедност ИКТ система у случају размене података**

**Члан 30.**

Подаци који су означени ознаком тајности, размењују се са другим органима, организацијама или правни лицима у складу са потписаним актом о размени података.

Акт из става 1. овог члана садржи податке о овлашћеним лицима за размену података, начину размене података, правни оквир за такву врсту размене, као и правни оквир којим се дефинише заштита података који се размењују.

**Учешће трећих лица у пословима ИКТ система**

**Члан 31.**

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Оператору, регулише се међусобно закљученим уговором.

Надлежни субјект ИКТ система је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

**Члан 32.**

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ.

Надлежни субјект ИКТ система је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

**Члан 33.**

Надлежни субјект ИКТ система је одговоран за надзор над поштовањем уговорених обавеза од стране трећих лица-пружаоца услуга у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система.

**Превентивне мере и реаговање на безбедносне инциденте**

**Члан 34.**

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, корисник ИКТ система је дужан да одмах обавести надлежног субјекта ИКТ система.

По пријему пријаве става 1. овог члана, надлежни субјект ИКТ система је дужан да одмах обавести директора и предузме мере у циљу заштите ресурса ИКТ система.

**Члан 35.**

Уколико се ради о инциденту који је дефинисан Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значај („Сл. гласник РС“бр. 94/16), надлежни субјект ИКТ система је дужан да обавести директора који о инциденту обавештава надлежни орган дефинисан наведеном Уредбом.

Надлежни субјект ИКТ система 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.

## *V Мере у циљу обезбеђења континуитета обављања посла у ванредним околностима*

**Члан 36.**

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде ЈКП Путеви Рашка, надлежни субјект ИКТ система је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди директор предузећа.

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.

## *VI Провера ИКТ система*

**Члан 37.**

Проверу ИКТ система врши надлежни субјект ИКТ система.

**Члан 38.**

Провера ИКТ система се врши тако што се:

1) проверава 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;

2) 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 директору предузеће.

**Члан 39.**

Извештај из члана 38. овог правилника садржи:

1) назив Оператора;

2) време провере;

3) податке о лицима која су вршила проверу;

4) извештај о спроведеним радњама провере;

5) закључке по питању усклађености Правилника 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.

## *VII Дисциплинска одговрност*

**Члан 40.**

Непоштовање одредби овог правилника представља повреду радних обавеза и повлачи законску одговорност корисника информатичких ресурса ИКТ система Оператора.

**Члан 41.**

Свако коришћење ИКТ ресурса Оператора ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

**Члан 42.**

Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже може се одузети право приступа.

## *VIII Прелазне и завршне одредбе*

**Члан 43.**

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли ЈКП Путеви Рашка.

**ЈКП ПУТЕВИ РАШКА**
Бр: 1/85-6 од 27.01.2021.год.

**НАДЗОРНИ ОДБОР**
Председник
Радомир Петровић, дипл.инж.маш.