СЛУЖБЕНИ ГЛАСНИК ОПШТИНЕ ДЕСПОТОВАЦ

2020.

ГОДИНА XV **БРОЈ 23** **ДЕСПОТОВАЦ 10.11.2020. године**

Цена овог броја је 200,00 динара. **Годишња претплата је 1.500,00 динара**

На основу члана 41. став 3. Закона о заштити података о личности („Сл. гласник РС“, бр. 87/18) и члана 38. Одлуке о Општинској управи ("Службени гласник општине Деспотовац бр. број 1/2017-пречишћен текст, 3/17, 9/17 и 9/19), начелник Општинске управе Деспотовац, доноси

П Р А В И Л Н И К
О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ У ОПШТИНСКОЈ УПРАВИ ДЕСПОТОВАЦ

I. ОСНОВНЕ ОДРЕДБЕ

Предмет правилника

Члан 1.

Правилником о заштити података о личности ближе се уређују обавезе Општинске управе у погледу заштите података о личности, уређују се техничке, организационе и кадровске мере, којима се обезбеђује заштита података о личности, уређује се начин вођења евиденција о збиркама података о личности, ближе се уређују права и обавезе лица за заштиту података о личности, ближе се уређује поступак остваривања права лица, чији се подаци о личности обрађују, као и начин пружања информација о подацима о личности које Општинска управа Деспотовац обрађује у вези са обављањем послова из своје надлежности.

Циљ доношења Правилника

Члан 2.

Циљ доношења овог Правилника је да се, у складу са начелом одговорности, регулишу интерна правила којима се обезбеђује да се обрада података о личности у Општинској управи, врши у складу са одредбама Закона о заштити података о личности („Сл. гласник РС“, бр. 87/18, у даљем тексту: Закон) и начелима законитости, поштења, транспарентности, ограничености сврхе обраде, минимизације података, тачности и ажурности података, ограниченог чувања података, интегритета и поверљивости.

Подаци о личности који се обрађују

Члан 3.

Општинска управа обрађује податке о личности лица, која учествују у било ком својству у управним и другим поступцима, који се воде пред Општинском управом, корисника административних и других услуга, запослених и чланова њихових породица,

лица ангажованих ван радног односа, бивших запослених и пензионера и посетилаца објеката које користи Општинска управа као и други Органи општине.

Општинска управа обрађује податке о личности корисника услуга у обиму који је неопходан за вршење надлежности из свог делокруга и поверених послова у циљу спровођења контроле и адекватног поступања по свим захтевима лица на које се подаци односе, у циљу вођења поступака јавних набавки, ради покретања и вођења спорова, у циљу евиденције поднетих захтева и у друге сврхе које су у директној вези са обављањем својих надлежности.

Општинска управа обрађује податке о личности запослених и чланова њихових породица, лица ангажованих ван радног односа, бивших запослених и пензионера ради извршења правних обавеза које општина као послодавац има у складу са Законом о запосленима у аутономним покрајинама и јединицама локалне самоуправе, другим прописима из области рада, пензијског, инвалидског, здравственог и социјалног осигурања, пореским и рачуноводственим прописима и прописима из области безбедности и здравља на раду и у друге сврхе, које су у директној вези са радом или ангажовањем лица ван радног односа.

Подаци запослених и других радно ангажованих лица се такође обрађују у мери у којој је то потребно ради закључења и извршења одговорајућих уговора са овим лицима.

Општинска управа обрађује податке о личности лица који као посетиоци улазе у пословне просторије и објекте које користи Општинска управа и други Органи општине и води евиденције о овим посетама у циљу заштите безбедности имовине и лица.

Правни основ обраде података о лнчности

Члан 4.

Правни основ за обраду података о личности су важећи закони, којима је регулисана одређена област у зависности од категорије лица на коју се односе подаци о личности, и то:

1) за обраду података о личности учесника у управном поступку правни основ је Закон о општем управном поступку и закони којима су уређени посебни управни поступци;
2) за обраду података понуђача-физичких лица и предузетника у поступцима јавних набавки правни основ је Закон о јавним набавкама;
3) за обраду података о личности службеника и намештеника у Општинској управи и лица ангажованих ван радног односа правни основ је Закон о запосленима у аутономним покрајинама и јединицама локалне самоуправе, Закон о раду, Закон о евиденцијама у области рада, Закон о здравственом осигурању, Закон о пензијском и инвалидском осигурању, Закон о порезу на доходак грађана, Закон о доприносима за обавезно социјално осигурање, Закон о државним и другим празницима у Републици Србији, Закон о безбедности и здрављу на раду, Закон о заштити од пожара, Закон о приватном обезбеђењу, Закон о одбрани, Закон о војној, радној и материјалној обавези, Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, Закон о рачуноводству, Закон о ревизији;
4) за обраду података о личности посетилаца који улазе у пословне просторије и објекте које користи Општинска управа и други Органи општине правни основ је Закон о приватном обезбеђењу;
5) податке о личности за чију обраду Општинска управа нема законско овлашћење прикупљаће на основу пристанка датог у складу са Законом.

Начела обраде података о личности

Члан 5.

Подаци о личности који се обрађују у Општинској управи морају:

1) се обрађивати законито, поштено и транспарентно у односу на лице на које се

подаци односе;

2) се прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама;
3) бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде;
4) бити тачни и ажурни;
5) се чувати у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде;
6) се обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера.

Законитост обраде

Члан 6.

Законита обрада је обрада која се врши у складу са законским и подзаконским прописима којима је регулисана заштита података о личности, односно другим законом којим се уређује обрада и ако је испуњен један од следећих услова:

1) обрада се врши у циљу вршења надлежности Општинске управе;
2) обрада се врши у циљу остваривања јавних интереса осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се односе подаци, а посебно ако је лице на које се подаци односе малолетно лице;
3) обрада се врши у циљу заштите животно важних интереса лица на које се подаци односе или другог лица;
4) лице на које се подаци односе је дало пристанак на обраду.

Пристанак лица на обраду података

Члан 7.

Пристанак лица на обраду података о личности мора:

1) Бити дат на изричит, јасан и недвосмислен начин (нпр. потписивањем изјаве, тј. сагласности, путем чек-бокс система, попуњавањем формулара којим се захтевају подаци о личности и другим радњама којима се активно изражава сагласност за обраду података о личности, док ћутање лица ни у ком случају не може представљати пристанак лица);
2) Бити дат од лица које је способно да изрази вољу - претпоставља се да су пунолетна лица, осим лица лишених пословне способности, способна да изразе вољу, док је у погледу малолетних лица увек потребно проверити да ли је за обраду података у одређене сврхе неопходно прибавити пристанак родитеља, односно законског заступника);
3) Бити слободно дат (пристанак није слободно дат ако је лице на које се подаци односе изложено ризику од преваре, узнемиравања, принуде или других негативних последица пре него што је изразило своју вољу);

Бити дат на начин који обезбеђује доказ постојања сагласности лица за обраду података о личности кроз документовање пристанка, јер општинска управа мора бити у могућности да предочи да је лице пристало на обраду својих података о личности.

Опозив пристанка на обраду података

Члан 8.

Лице на које се подаци односе има право да опозове пристанак у сваком тренутку.

Опозив пристанка не утиче на допуштеност обраде која је вршена на основу пристанка пре опозива.

Пре давања пристанка лице на које се подаци односе мора бити обавештено о праву на опозив, као и дејству опозива.

Опозивање пристанка мора бити једноставно, као и давање пристанка.

Рок чувања пода така

Члан 9.

Рок чувања података о личности које обрађује Општинска управа може бити одређен законом или актом донетим на основу закона, уговором или самом сврхом и потребом обраде података.

Подаци о корисницима чувају се у року који је неопходан за остваривање сврхе обраде.

Подаци о запосленима чувају се трајно у складу са законом којим се уређују евиденције у области рада.

Податке који се обрађују искључиво на основу пристанка, Општинска управа ће обрађивати и чувати док се не оствари сврха обраде, односно до опозива пристанка.

II. ОБАВЕЗЕ ЗАПОСЛЕНИХ У ПОГЛЕДУ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ КОЈЕ ОБРАЂУЈУ

Поверљивост података

Члан 10.

Подаци о личности који се обрађују у Општинској управи сматрају се поверљивим и дужни су да их чувају сви запослени који на било који начин и по било ком основу за њих сазнају.

Запослени који дођу у контакт са подацима о личности из става I. не смеју их саопштавати, нити учинити доступним неовлашћеним лицима, како за време трајања уговора о раду или другог уговора ван радног односа, тако и по његовом престанку.

Нарушавање поверљивости као повреда радне обавезе

Члан 11.

Запослени су дужни да све податке о личности које Општнска управа обрађује, чувају у складу са Законом, овим Правилником и међународним стандардима и процедурама који су имплементирани у Општинској управи у области заштите и безбедности информација, уз примену свих расположивих техничких и организационих мера.

Непоштовање обавеза прописаних Законом и овим Правилником сматра се повредом радне обавезе и представља разлог за престанак радног односа службеника, отказ уговора о раду намештеника или једнострани раскид уговора ван радног односа по основу кога је лице ангажовано.

Приликом уручивања одговарајућег решења којим се заснива радни однос са службеником у Општинској управи, потписивања уговора о раду са намештеником или уговора ван радног односа, службеник за људске ресурсе упознаје новозапосленог с овим Правилником и обавезом чувања и заштитом података о личности.

Лица овлашћена за обраду података о личности

Члан 12.

Обраду података о личности у име Општинске управе могу спроводити искључиво лица која су за то овлашћена, и то:

1) решењем о распоређивању или уговором ван радног односа у обиму у ком је обрада података о личности неопходна ради извршења обавеза ових лица према Општинској управи;
2) посебним актом који доноси општинско веће или начелник управе у обиму дефинисаним тим актом.

Лица која су овлашћена за обраду података о личности у име Општинске управе дужна су да их обрађују искључиво у сврху због које им је омогућен приступ тим подацима и само у обиму у ком је овлашћен за обраду.

Обавезе лица овлашћених на обраду личности

Члан 13.

Лица која су овлашћена за обраду података о личности у име Општинске управе дужна су да поштују следећа правила:

1) забрањено је правити резервне копије података на локални диск рачунара, екстерну меморију, приватни рачунар, меморију мобилног телефона или виртуалну меморију („cloud“);
2) обавезно је коришћење лозинки приликом приступа подацима и оне не смеју бити подељене са неовлашћеним лицима;
3) обавезно је излоговање („закључавање“) радне станице пре сваког, чак и краткотрајног, удаљавања са радног места;
4) забрањено је заустављање рада или брисање антивирусног програма, мењање подешених опција или самовољно инсталирање другогог антивирусног програма;
5) забрањено је инсталирање софтвера или хардвера без одобрења овлашћеног лица;
6) подаци се не смеју откривати неовлашћеним особама, ни запосленима у Општинској управи који нису овлашћени за приступ тим подацима, ни лицима ван Општинске управе;
7) подаци се морају редовно прегледати и ажурирати;
8) подаци се морају обрисати, уколико њихово чување више није потребно;
9) подаци у физичком облику се не смеју држати на столу, остављати у фотокопир машини или на другим местима где може доћи до откривања и злоупотребе података;
10) запослени су дужни да затраже помоћ од свог непосредног руководиоца или Лица за заштиту података о личности уколико нису сигурни како поступити са подацима о личности;
11) обавезно је поштовање и примена свих мера заштите података о личности прописаних овим Правилником.

Под неовлашћеним откривањем и преношењем података који представљају податке о личности подразумева се како намерно или услед непажње откривање ових података, тако и откривање које је последица недовољне заштите ових података од стране лица које је овлашћено за обраду.

Обавезе руководиоца организационе јединице

Члан 14.

Руководилац организационе јединице у којој се врши обрада података о личности је дужан да утврди групе података или појединачне податке за сваку појединачну збирку података које је појединим запосленима у тој организационој јединици потребно учинити доступним ради обављања редовних послова, као и да утврди којим запосленима треба обезбедити само увид у податке, као и сврху тог увида.

Основни принцип којим се руководилац организационе јединице руководи приликом одређивања круга лица која ће имати приступ одређеним подацима о личности је принцип „минимално потребних права“, што подразумева да ће се приступ подацима и радње обраде свести на најмању могућу меру, односно меру неопходну за обављање послова тог лица.

Руководилац организационе јединице у којој се врши обрада података о личности је дужан да мапира, води и ажурира евиденције о збиркама података о личности чија обрада се врши у тој организационој јединици, као и да доставља све информације неопходне за обавештавање Поверенику и лица на које се подаци о личности односе.

III. ТЕХНИЧКЕ, ОРГАНИЗАЦИОНЕ И КАДРОВСКЕ МЕРЕ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ

Обавезе Општинске управе као руковаоца

Члан 15.

Општинска управа као руковалац подацима о личности, обезбеђује следеће мере заштите података о личности од неовлашћене или незаконите обраде, као и од случајног или незаконитог уништења или оштећења, губитка, измене, откривања, приступа подацима и сваке друге злоупотребе, и то:

1) опште мере заштите;
2) мере заштите од неовлашћеног приступа подацима о личности;
3) посебне мере заштите од неовлашћеног приступа просторијама у којима се чувају досијеи запослених у физичком облику и приступ сервер салама;
4) мере заштите од случајног губитка, уништења или оштећења података о личности:
5) мере заштите од недопуштеног објављивања и других злоупотреба података о личности.

Опште мере заштите

Члан 16.

У Општинској управи спроводе се опште мере заштите утврђене законским и подзаконским прописима и интерним актима, и то:

1) мере физичког и техничког обезбеђења имовине и лица, мере заштите од пожара, мере заштите архивске грађе;
2) организационе мере и радни процеси утврђени имплементираним стандардима и процедурама ради обезбеђивања тачности, ажурности и правилности обављања послова, спречавања неовлашћене измене документације и података, неовлашћеног приступа програмским апликацијама и другим средствима за рад и опреми.

Мере заштите података од неовлашћеног приступа подацима о личности

Члан 17.

Општинска управа спроводи следеће мере заштите од неовлашћеног приступа подацима о личности:

1) Надзор и контрола приступа објектима, односно просторијама у којима се налазе подаци о личности у физичком облику;
2) Приступ подацима у физичком облику осигуран је тако што се ови подаци чувају у ормарима или просторијама које се закључавају;
3) Приступ подацима о личности у електронском облику осигуран је посебном лозинком сваког запосленог који је овлашћен да врши обраду података о личности или да врши увид у податке о личности;
4) Информациони систем и програми заштићени су савременим системима заштите од малициозних програма, вируса и других радњи којима се може нарушити интегритет

и стабилност ових система;

5) Запослени су дужни да искључе или програмски закључају рачунар са подацима о личности у случају напуштања просторија у којима нема надзора других запослених и на крају радног времена.

Општинска управа спроводи и друге мере физичке и техничке заштите у посебним случајевима.

Посебне мере заштите од неовлашћеног приступа просторијама у којима се чувају досијеи запослених у физичком облику и приступ сервер салама

Члан 18.

Просторије у којима су смештени досијеи запослених, као и просторије у којима се налазе сервери на којима се складиште и чувају подаци (сервер сале) обезбеђују се посебним мерама заштите, и то:

1) овлашћени улазак и боравак у овим просторијама дозвољен је само запосленима који у њима обављају своје послове;
2) све остале особе и други запослени у наведене просторије могу ући и боравити у њима искључиво у присуству запослених особа овлашћених за боравак у овој просторији;
3) уколико нема никога у просторијама од запослених, као и након одласка с посла просторије се закључавају;
4) друге мере физичке и техничке заштите у посебним случајевима.

Мере из става 1. овог члана спроводе непосредно запослени, а спровођење мера контролишу непосредни руководиоци.

Мере заштите од случајног губитка, уништења или оштећења података о личности

Члан 19.

Општинска управа обезбеђује систем поновне расположивости и заштите интегритета података о личности кроз бекап базе података који се спроводи на крају радног дана, чиме се обезбеђује сигурност свих података похрањених у току радног дана и искључује могућност да се исти изгубе, оштете, избришу, неовлашћено измене, односно на било који други начин наруши њихов интегритет.

Мере заштите од злоупотреба података о личности

Члан 20.

Општинска управа може одлучити да, на основу дате сагласности Скупштине општине пренесе податке о личности трећем лицу на основу закона или на основу уговора.

У случају преношења података из става 1. начелник Општинске управе је дужан да лицу, коме се подаци преносе, у мери у којој је то могуће достави и информације које су неопходне за оцену степена тачности, потпуности, провереності односно поузданости података о личности, као и да му достави обавештење о ажурности тих података.

Преношење података државним органима

Члан 21.

Општинска управа може пренети одређене податке надлежним државним органима ради испуњења својих законских обавеза и остваривања права, као и остваривања права запослених и лица ангажованих ван радног односа.

Податке о личности запослених и лица ангажованих ван радног односа Општинска управа доставља у складу са законским обавезама према прописима из области рада и

радних односа, пореским, рачуноводственим прописима надлежним органима као што су: Министарство финансија - Пореска управа, Министарство рада, Републички фонд за пензијско и инвалидско осигурање, Републички фонд за здравствено осигурање, Министарство одбране, ревизорски органи и институције.

У случајевима законом прописане размене података о личности са надлежним државним органима примењују се Закон и законски прописи из области у којој се размена података обавља.

Преношење података о личности на основу уговора

Члан 22.

Општина може пренети одређене податке о личности на основу уговора са трећим лицем, као обрађивачем, ради обављања послова из своје надлежности и рационалнијег управљања буџетским и људским ресурсима, а која су ангажована да врше поједине радње обраде података о личности за рачун и у име јединице локалне самоуправе.

Општина ће сваки однос који подразумева поверавање одређених радњи обраде другом лицу као обрађивачу регулисати посебним уговором о обради података, који је закључен у писаном облику, што обухвата и електронски облик.

Општина може да закључи уговор из става 1. овог члана само са оним лицем које у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама Закона и да се обезбеђује заштита права лица на која се подаци односе.

Уговор из става 1. овог члана обавезно садржи следеће одредбе:

1) обавезу обрађивача да обрађује податке само у оквиру добијеног овлашћења, осим ако је обрађивач законом обавезан да обрађује податке;
2) обавезу обрађивача да користи податке искључиво у сврхе које су уговорене;
3) права лица на која се подаци односе;
4) обавезу обрађивача и општине као руковаоца да обезбеде организационе и техничке мере заштите података;
5) обавезу обрађивача да помаже општини као руковаоцу у испуњавању обавеза руковаоца у односу на захтеве за остваривање права лица на које се подаци односе;
6) обавезу обрађивача да поштује услове за поверавање обраде другом обрађивачу;
7) запослени и друга лица ангажована код обрађивача имају обавезу чувања поверљивости података;
8) обавезу обрађивача да учини доступним општини као руковаоцу све информације које су неопходне за предочавање испуњености обавеза обрађивача, као и информације које омогућавају и доприносе контроли рада обрађивача, који спроводи руковалац или друго лице;
9) обавезе које обрађивач има по окончању уговорене обраде података.

Изношење података ван територије Републике Србије

Члан 23.

Подаци о личности којима управља Општинска управа не износе се ван територије Републике Србије.

IV. ЕВИДЕНЦИЈЕ О ОБРАДИ ПОДАТАКА О ЛИЧНОСТИ

Садржина збирки података о личности

Члан 24.

Свака организациона јединица у којој се обрађују подаци о личности води евиденцију свих збирки података које настају и воде се у тој организационој јединици.

Евиденција из става 1. овог члана води се у електронском облику.

За сваку појединачну збирку података о личности утврдиће се: назив организационе јединице која врши обраду података о личности, назив збирке података, податке о личности који се обрађују, да ли се обрађује посебна врста података о личности и која, да ли се обрађују подаци о личности малолетних лица, категорија лица на коју се подаци односе, правни основ обраде података, односно успостављања збирке података, сврха обраде података о личности, да ли се подаци преносе трећим лицима, ко има приступ збирци података о личности, начин прикупљања података о личности, начин обраде података о личности, предузете мере заштите збирке података, рок чувања података.

Збирке података о личности успостављаће се, мењати и брисати у складу са законским одредбама и потребама вршења надлежности Општинске управе.

Достављање података Лицу за заштиту података о личности

Члан 25.

Организациона јединица која води збирку података о личности дужна је да достави Лицу за заштиту података о личности податке о евиденцији у року од 3 радна дана од дана формирања збирке података или промене у постојећој збирци.

Организациона јединица је дужна да ажуриране евиденције о збиркама података које се воде у тој организационој јединици доставља на захтев Лица за заштиту података о личности.

Лице за заштиту података о личности дужно је да води евиденцију о свим збиркама података које се воде у свим организационим јединицама у општинској управи.

Евиденција о активностима обраде

Члан 26.

У организационим јединицама у којима се обрађују подаци о личности обавезно се води евиденција о активностима обраде, а о преносу података трећим странама мора бити обавештено Лице за заштиту података о личности, коме се и достављају подаци из евиденција.

Евиденција о активности обраде садржи следеће информације:

1) име и презиме и контакт податке лица које је задужено за евиденцију у организационој јединици;
2) категорију личних података;
3) да ли се ради о посебној врсти података;
4) категорија лица на које се подаци односе;
5) сврха обраде;
6) коме је извршен пренос података;
7) ко има приступ подацима;
8) предвиђене мере заштите;
9) потпис одговорне особе.

V. ЛИЦЕ ЗА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ

Именовање Лица за заштиту података о личности

Члан 27.

Начелник општинске управе посебном Одлуком именује Лице за заштиту података о личности.

Лице за заштиту података о личности одређује се на основу његових стручних квалификација, а нарочито стручног знања и искуства из области заштите података о личности, као и способности за извршавање обавеза из Закона.

Лице за заштиту података о личности може да обавља друге послове из делокруга организационе јединице у којој је систематизовано његово радно место, а начелник Општинске управе је у обавези да обезбеди да извршавање других послова и обавеза не доведе Лице за заштиту података о личности у сукоб интереса.

За извршавање обавеза из Закона Лице за заштиту података о личности непосредно је одговорно начелнику Општинске управе.

Дужности Лица за заштиту података о личности

Члан 28.

Лице за заштиту података о личности има следеће обавезе:

1) информише и даје мишљење начелнику Општинске управе, руководиоцима других органа, као и запосленима који врше радње обраде о њиховим законским обавезама у вези са заштитом података о личности;
2) прати примену одредби Закона, других закона и интерних прописа који се односе на заштиту података о личности, укључујући и питања поделе одговорности, подизања свести и обуке запослених који учествују у радњама обраде, као и контроле;
3) даје мишљење, када се то затражи, о процени утицаја обраде на заштиту података о личности и прати поступање по тој процени;
4) сарађује са Повереником, представља контакт тачку за сарадњу са Повереником и саветује се са њим у вези са питањима која се односе на обраду.

VI. ОСТВАРИВАЊЕ ПРАВА ЛИЦА ЧИЈИ СЕ ПОДАЦИ О ЛИЧНОСТИ ОБРАЂУЈУ

Права лица чији се подаци о личности обрађују

Члан 29.

Лице на које се подаци односе има право да од Општинске управе захтева информацију о томе да ли обрађује његове податке о личности, приступ тим подацима, као и информације прописане Законом.

Лице на које се подаци односе има право да од Општинске управе захтева да се његови нетачни подаци о личности без непотребног одлагања исправе, односно да се у зависности од сврхе обраде, непотпуни подаци о личности допуне.

Лице на које се подаци односе има право на брисање података о личности под условима прописаним Законом.

Лице на које се подаци односе има право да се обрада његових података о личности ограничи ако је испуњен један од случајева прописаним Законом.

Лице на које се подаци односе има право право на преносивост података под условима прописаним Законом.

Лице на које се подаци односе има право да се на њега не примењује одлука донета искључиво на основу аутоматизоване обраде, укључујући и профилисање, ако се том одлуком производе правне последице по то лице или та одлука значајно утиче на његов положај, у складу са Законом.

Лице на које се подаци односе има право право на информацију о томе да ли је давање података о личности законска или уговорна обавеза или је давање података неопходан услов за закључење уговора, као и о томе да ли лице на које се подаци односе има обавезу да да податке о својој личности и о могућим последицама ако се подаци не дају.

Уколико се обрада заснива на пристанку, лице на које се подаци односе има право да опозове пристанак у сваком тренутку.

Лице на које се подаци односе има право да поднесе притужбу Поверенику, ако сматра да је обрада података о његовој личности извршена супротно одредбама Закона.

Подношење притужбе Поверенику не утиче на право овог лица да покрене друге поступке управне или судске заштите.

Примена прописа у поступку остваривања права лица чији се подаци о личности обрађују

Члан 30.

Захтеви за остваривање права лица на које се подаци о личности односе достављају се Лицу за заштиту података о личности.

У поступку за остваривање права лица чији се подаци о личности обрађују, Лице за заштиту података о личности примењује одредбе Закона и овог Правилника.

Поступак остваривања права лица чији се подаци о личности обрађују

Члан 31.

Лице за заштиту података о личности ће приликом поступања по захтеву лица на које се подаци о личности односе најпре потврдити идентитет подносиоца захтева и утврдити да се захтев односи на то лице.

Ради провере идентитета подносиоца захтева Лице за заштиту података о личности може захтевати од подносиоца и додатне информације.

Руководиоци организацоних јединица у којој се обрађују подаци о личности дужни су да, на захтев Лица за заштиту података о личности, пруже све расположиве информације од значаја за поступање по захтеву за остваривање права лица чији се подаци о личности обрађују, без одлагања.

Лице за заштиту података о личности је дужно да, најкасније у року од 30 дана од дана пријема захтева, пружи информације о поступању лицу на које се подаци односе.

Уколико је лице на које се подаци односе захтев поднело електронским путем, информације се такође морају пружити електронским путем ако је то могуће, осим уколико лице не захтева да се информације пруже на други начин.

Узимајући у обзир сложеност и број захтева, рок из става 1. овог члана може бити продужен за још 60 дана уколико је то неопходно, у ком случају се о продужењу рока и разлозима за продужење рока лице на које се подаци о личности односе мора обавестити у року од 30 дана од дана пријема захтева.

У случају непоступања по захтеву у роковима описаним овим чланом, лице на које се подаци о личности односе мора се најкасније у року од 30 дана од дана пријема захтева обавестити о разлозима за непоступање по захтеву, као и о праву на подношење притужбе Поверенику за информације од јавног значаја и заштиту података о личности, односно тужбе суду.

Обавеза пружања информација без накнаде

Члан 32.

Информације којима се омогућава остваривање права лица пружају се без накнаде, осим у случају када је захтев лица очигледно неоснован или претеран, а посебно ако се исти захтев учестало понавља, када се могу наплатити нужни административни трошкови пружања информације или одбити поступање по захтеву.

VII. ОБАВЕШТАВАЊЕ О ОБРАДИ И ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ

Члан 33.

Општинска управа ће објавити на интернет страници и редовно ажурирати опште информације о заштити података о личности о следећим подацима:

1) контакт подацима Лица за заштиту података о личности;
2) сврси обраде података о личности;
3) правном основу обраде података о личности;
4) примаоцима података о личности;
5) року чувања података о личности;
6) правима лица чији се подаци о личности обрађују.

VIII. ЗАВРШНЕ ОДРЕДБЕ

Члан 34.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли Општинске управе Деспотовац и биће објављен у Службеном гласнику општине Деспотовац.

ОПШТИНСКА УПРАВА ДЕСПОТОВАЦ
Број: 02-86/2020-04 од 30.10.2020. године

НАЧЕЛНИК
ОПШТИНСКЕ УПРАВЕ
Гордана Јаблановић, дипл.правник с.р.

На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16, 94/17 и 77/19), члана 2. Уредбе о ближем садржају акта 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) и члана 38. Одлуке о Општинској управи ("Службени гласник општине Деспотовац бр. број 1/2017-пречишћен текст, 3/17, 9/17 и 9/19), начелник општинске управе Деспотовац доноси,

ПРАВИЛНИК
о безбедности информационо - комуникационог система Општинске управе Деспотовац

I. Уводне одредбе

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности и Уредбом 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, утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационих система (у даљем тексту: информациона безбедност), као и овлашћења и одговорности у вези са

информационом безбедношћу и ресурсима ИКТ система Општинске управе Деспотовац (у даљем тексту: ИКТ систем).

Под информационо-комуникационим системом који је предмет заштите од безбедносних ризика подразумевају се електронске комуникационе мреже, електронски уређаји на којима се чува и врши обрада података коришћењем рачунарског програма, оперативни и апликативни рачунарски програми, програмски код, подаци који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациона структура путем које се управља ИКТ системом, кориснички налози, тајне информације за проверу веродостојности као и техничка и корисничка документација.

Члан 2.

Циљеви доношења Правилника су:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа информационе безбедности Општинске управе Деспотовац;
2. спречавање и ублажавање последица инцидената, којима се угрожава или нарушава информациона безбедност;
3. подизање свести код доносилаца одлука, посебно шефова одељења и служби Општинске управе Деспотовац и запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4. прописивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система;
5. свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите у Општинској управи Деспотовац.

Члан 3.

Мере прописане овим Правилником служе превенцији од настанка инцидената и минимизацији штете од инцидената и примењују се у свим организационим јединицама Општинске управе Деспотовац, према посебном закону, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Општинске управе Деспотовац.

Запослени у Општинској управи Деспотовац у свим одељењима и службама потписују изјаву да су упознати са одредбама овог Правилника. Један примерак ове изјаве се чува у персоналном досијеу запосленог, са јасно видљивим датумом потписивања.

За праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама одговорни су начелник Општинске управе Деспотовац и шеф Одељења за општу управу и послове органа општине као руководилац основне организационе јединице у чијем су делокругу ИКТ послови.

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.

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Општинске управе Деспотовац

Члан 5.

Општинска управа Деспотовац у оквиру организационе структуре утврђује послове и одговорности руководилаца и запослених у циљу управљања информационом безбедношћу.

Правилником о унутрашњој организацији и систематизацији радних места утврђују се радна места на којима се обављају послови од значаја за обезбеђивање и праћење безбедности информационог система у Општинској управи Деспотовац као и степен обуке и квалификација запослених и нивои приступа информационим ресурсима.

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 Општинске управе Деспотовац надлежан је начелник Општинске управе и шеф Одељења за општу управу и послове органа општине као руководилац основне организационе јединице у чијем су делокругу ИКТ послови.

Члан 6.

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 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 Општинске управе Деспотовац, 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 Шеф Одељења за општу управу и послове органа општине, обавештава начелника Општинске управе, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

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

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

Члан 8.

Начелник Општинске управе Деспотовац 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. Њихове одговорности се утврђују процедуром о правима приступа информационом систему, решењем о распоређивању на одређено радно место (за службенике), уговором о раду (за намештенике), посебним уговорима (о привременим и повременим пословима и сл.) за радно ангажована лица по другом основу и споразумом о поверљивости.

Руководилац организационе јединице надлежне за ИКТ и службеници који управљају ИКТ системом се процедуром о правима приступа информационом систему и решењем о распоређивању овлашћују за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

У поступку заснивања радног односа за запослене који управљају ИКТ системом односно запослене који користе ИКТ систем у Општинској управи Деспотовац се проводе радње у циљу провере испуњености услова сразмерно пословним захтевима, класификацији информација којима се на радном месту које се попуњава одобрава приступ и сагледаним ризицима.

Сви запослени и радно ангажована лица по другом основу, којима је додељен приступ поверљивим информацијама, морају потписати споразум о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Програмима стручног усавршавања у Општинској управи Деспотовац се обезбеђује да се запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура у области информационе безбедности континуирано обучавају у циљу унапређења техничког и технолошког знања. Сви службеници Општинске управе Деспотовац су у обавези да заврше одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и у примени у Општинској управи Деспотовац. Дисциплински поступак се покреће по предлогу начелника Општинске управе односно шефова одељења и служби.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања. Дужности и обавезе које остају важеће и после престанка ангажовања су садржане у тексту решења о распоређивању, уговора о раду, односно уговора о ангажовању лица ван радног односа.

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

Члан 9.

За поступања приликом престанка запослења или ангажовања задужен је Шеф Службе за заједничке послове и управљање људским ресурсе у сарадњи са службеницима који управљају ИКТ системом који предузимају следеће активности:

1) проверавају испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату;
2) прегледају све налоге и приступе систему који су били доступни службенику односно намештенику, преузимају од њега електронске и друге мобилне уређаје;
3) проверавају враћене мобилне уређаје и уређаје за преношење података;
4) дају налог за укидање налога електронске поште и свих других права приступа систему на дан престанка радног односа или другог основа ангажовања;
5) прегледају све налоге за приступ и прикупљају приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
6) преузимају картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми.

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра Општинске управе Деспотовац су сви ресурси који садрже пословне информације Општинске управе Деспотовац, 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 Одељење за општу управу и послове органа општине, у папирној или електронској форми.

У складу са Законом о буџетском рачуноводству, Уредбом о буџетском рачуноводству и Правилником о унутрашњем уређењу и систематизацији радних места, надлежна организациона јединица за буџет и финансије у сарадњи са службеницима који управљају ИКТ системом врши идентификацију имовине која је предмет заштите и документује њен животни циклус.

Предмет заштите су:

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

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

Члан 11.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем. Класификациона шема поверљивости информација је заснована на четири нивоа:

1) откривање не изазива никакву штету;
2) откривање изазива мању непријатност или мању штету;
3) откривање има значајан краткорочни утицај на обављање послова из делокруга Општинске управе Деспотовац;
4) откривање има озбиљан утицај на дугорочне стратешке циљеве или обављање послова из делокруга Општинске управе Деспотовац.

Општинска управа Деспотовац врши класификацију ради:

1) јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење;
2) подизања свести о вредности информације или документа;
3) заштите података у покрету ради боље и интелигентније интеграције са DLP, WEB gateway и осталим производима за заштиту параметара и крајњих уређаја.

Подаци који се налазе у ИКТ систему представљају тајну, ако су тако дефинисани одредбама посебним прописима.

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 55/05, 71/05 – исправка, 101/07, 65/08 и 16/11).

Детаљан опис информација, носачима информација и доступности података налази се у Информатору о раду Општинске управе Деспотовац.

7. Заштита носача података

Члан 12.

Одељење за општу управу и послове органа општине, ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да:

- подаци и документи (посебно они са ознаком тајности) 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 обезбеђено одлуком начелника.
- подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника (ит техничар, начелник, администратор, шеф одељења).

Евиденцију носача на којима су снимљени подаци, води Одељење за општу управу и послове органа општине и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, начелник Општинске управе ће одредити одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на медијима, подаци морају бити неповратно обрисани, а ако то није могуће, такви медији 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 у складу са архитектуром ИКТ система и домена безбедног и примереног 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 процесирају у оквиру информатичких ресурса власништво Општинске управе Деспотовац 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) захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8) обезбеди сигурност података у складу са важећим прописима;
19) 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) на радној станици не сме да складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (backup) података у складу са прописаним процедурама;

13) користи интернет и електронску пошту у Општинској управи Деспотовац у складу са прописаним процедурама;
14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, 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 (анти вирус 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, осим ако то није склопу одржавања система или отклањања проблема, уз сагласност надређеног.

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 за управљање доменом и базама података може да користи само запослени распоређен на пословима ит техничара у Одељењу за општу управу и послове органа општине.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу кога се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налози су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности. Кориснички налог додељује администратор, на основу захтева Шефа Службе за заједничке послове и управљање људским ресурсима задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима, а у складу са потребама обављања пословних задатака од стране запосленог-корисника. Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева Шефа Службе за заједничке послове и управљање људским ресурсима, односно надлежног руководиоца.

Коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење. Корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички налози. Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима. Администратор ИКТ система сваких 12 месеци врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај запослења).

Редовне пословне активности се не врше из привилегованих корисничких налога. Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

(Пример:Корисничко име се креира по матрици име.презиме, латиничним писмом без употребе слова ђ,ж,љ, њ, ћ, ч, џ, ш.

(Препорука: Уместо ових слова користити слова из табеле.)

Ћирилична слова	Латинична слова
Ђ	dj
Ж	z
Љ	lj
Њ	nj
ћ, ч	c
Ш	s
Џ	dz

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

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

Ако запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Запослени-корисник је дужан да мења лозинку најмање једном у шест месеци.

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

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 16.

Приступ ресурсима ИКТ система Општинске управе Деспотовац не захтева посебну криптозаштиту.

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

Запослени на пословима ИКТ су задужени за инсталацију потребног софтвера и хардвера за коришћење сертификата.

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

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

Члан 17.

У Општинској управи Деспотовац се обезбеђује и примењује одговарајућа контрола приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава. Такође, безбедним конфигурисањем се онемогућава приступ кључној опреми а у циљу спречавања видљивости поверљивих информација, активностима споља.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује са као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом и видео надзором.

Простор административне зоне је обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор).

Евиденцију о уласку у ову зону води Одељење за општу управу и послове органа општине.

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

Члан 18.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система и запосленима на пословима ИКТ.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу начелника Општинске управе, и уз присуство надлежног лица распоређеног на пословима администратора и шефа Одељења за општу управу и послове органа општине.

Приступ административној зони може имати и запослена на пословима одржавања хигијене уз присуство надлежног лица распоређеног на пословима администратора и шефа Одељења за општу управу и послове органа општине.

Просторија мора бити видљиво обележена и у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима.

Врата на овој просторији морају увек бити затворена.

Сервери и активна мрежна опрема (switch, modem, router, firewall), 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.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења начелника.

У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење начелника који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења начелника Општинске управе, 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 мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Општинске управе Деспотовац.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

Запослени на пословима ИКТ 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 начелнику Општинске управе одговарајуће мере.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву 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 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 средства за обраду података од злонамерног софтвера

Члан 20.

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 меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски у 7 сати врши допуна антивирусних дефиниција.

Сваког претпоследњег радног дана (четвртка) у недељи је потребно оставити укључене и закључане рачунаре ради скенирања на вирусе.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса.

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 циљу заштите, односно упада у ИКТ систем Општинске управе Деспотовац са интернета, запослени распоређен на пословима администратора у Одељењу за општу управу и послове органа општине је дужан да одржава систем за спречавање упада.

Шефови одељења и служби одређују који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему Одељење за општу управу и послове органа општине може укинути приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени-корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши Одељење за општу управу и послове органа општине.

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

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Одељењу за општу управу и послове органа општине.

Строго је забрањено гледање филмова и играње игрица на рачунарима и "крстарење" WEB страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

Недозвољена употреба интернета обухвата:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ 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 друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимање (download) података велике “тежине” које проузрокује “загушење” на мрежи;
- преузимање (download) материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

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

Члан 21.

Листа провера које се спроводе у циљу заштите од злонамерног софтвера обухвата али се не ограничава на:

а) проверу, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер;

б) проверу, пре коришћења, садржаја прилога електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер; ова провера се спроводи на разним местима, нпр. на серверима за електронску пошту, на стоним рачунарима или приликом уласка у мрежу оператора ИКТ система;

в) проверу постојања злонамерних софтвера на веб-страницама;

г) обука за извештавање и опоравак од напада злонамерним софтвером;

д) припрему одговарајућих планова за континуитет пословања приликом опоравка од напада злонамерним софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак;

ђ) имплементацију процедура за редовно прикупљање информација, као што је претплата на адресне спискове за доставу или провера веб-страница на којима се дају информације о новим злонамерним софтверима;

е) имплементацију процедура за верификовање информација о злонамерним софтверима и обезбеђење да су упозоравајући извештаји тачни и информативни; за разликовање лажних од стварних злонамерних софтвера користе се квалификовани извори, нпр. проверени часописи, поуздане странице на Интернет мрежи или испоручиоци програма против злонамерних софтвера.

16. Заштита од губитка података

Члан 22.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују. Заштитне копије корисницима обезбеђују корисничке податке, функционалност

сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

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

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система. За чување заштитних копија користе се магнетне траке, екстерни хард дискови и CD/DVD медији.

Дневно копирање-архивирање врши се за сваки радни дан у седмици, од 20 часова сваког радног дана.

Недељно копирање-архивирање врши се последњег радног дана у недељи, од 21 час.

Месечно копирање-архивирање врши се последњег радног дана у месецу, за сваки месец посебно, од 22 часа.

Годишње копирање-архивирање врши се последњег радног дана у години.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе („Сл. гласник РС“, бр 10/93, 14/93-испр, 67/2016 и 3/2017).

Сваки примерак преносног информатичког медија са копијама-архивама, мора бити означен бројем, врстом (дневна, недељна, месечна, годишња), датумом израде копије-архиве, као и именом запосленог-корисника који је извршио копирање-архивирање.

Дневне, недељне и месечне копије-архиве се чувају у безбедносној зони.

Годишње копије-архиве се израђују у два примерка, од којих се један чува у просторији у којој се чувају дневне, недељне и месечне копије-архиве а други примерак у згради Архиве Општинске управе Деспотовац.

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

Члан 23.

О активностима администратора и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др).

Сваког последњег радног дана у недељи датотеке у којима се налази дневник активности се архивирају по процедури за израду копија-архива осталих података у ИКТ систему, у складу са чл. 20 овог правилника.

18. Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Општинске управе Деспотовац, односно Freeware и Opensource верзије.

Инсталацију и подешавање софтвера може да врши само запослени у Одељењу за општу управу и послове органа општине, односно запослени-корисник који има овлашћење за то.

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

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.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

Одељење за општу управу и послове органа општине најмање једном месечно а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, запослени у Одељењу за општу управу и послове органа општине је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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

Члан 26.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност начелника Општинске управе.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 27.

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) се мора налазити у закључаном rack орману.

Запослени у Одељењу за општу управу и послове органа општине је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Бежична мрежа коју могу да користе посетиоци објеката у надлежности Општинске управе, мора бити одвојена од интерне мреже коју користе корисници запослени у Општинској управи и кроз коју се врши размена службених података.

Та мрежа треба да буде означена (ССИД) по моделу Општинска управа Деспотовац.

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

Члан 28.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Општинској управи, биће дефинисан уговором који ће бити склопљен са тим лицима.

Запослени у Одељењу за општу управу и послове органа општине је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система запослени у Одељењу за општу управу и послове органа општине води документацију.

Документација из претходног става мора да садржи описе свих процедура а посебно процедура које се односе на безбедност ИКТ система.

23. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 29.

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.

Шеф Одељења за општу управу и послове органа општине је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

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 Општинске управе Деспотовац као уговорне стране, а за потребе извршења предмета преговора.

Изјава о поверљивости, односно уговор о пружању услуга, садржи одредбу о поверљивости са јасно утврђеном обавезом и одговорношћу пружаоца услуге уз претњу раскида уговора и накнаде штете у корист Општинске управе Деспотовац у случају повреде ове одредбе.

Изјава о поверљивости обавезно гласи:

“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.

Свака уговорна страна се обавезује да податке и информације које јој буду учињене доступним у складу са овим уговором и обавезом извршења уговорених послова и обавеза, буду стављене на располагање и увид запосленима, уколико је то неопходно ради извршења обавеза из овог уговора.

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.”

Пружаоци услуга дужни су да захтеве Општинске управе Деспотовац у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе.

Шеф Одељења за општу управу и послове органа општине је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби правилника којима су такве активности дефинисане.

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

Члан 30.

Шеф Одељења за општу управу и послове органа општине је одговоран 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 уговорених обавеза Шеф Одељења за општу управу и послове органа општине је дужан да одмах обавести начелника, како би он могао да предузме мере у циљу отклањања неправилности.

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

Члан 31.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести Шефа Одељења за општу управу и послове органа општине.

По пријему пријаве Шеф Одељења за општу управу и послове органа општине је дужан да одмах обавести начелника Општинске управе и предузме мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, „Сл. Гласник РС“, бр, 94/2016), Шеф Одељења за општу управу и послове органа општине, је дужан да поред начелника обавести и надлежни орган дефинисан овом уредбом.

Одељење за општу управу и послове органа општине 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.

26. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 32.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Општинске управе, Одељење за општу управу и послове органа општине, је дужано 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.

Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује Одељење за општу управу и послове органа општине, и то у три примерка, од којих се један налази код њега, други код запосленог надлежног за послове одбране и ванредне ситуације а трећи примерак код начелника Општинске управе.

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

I. Измена Правилника о безбедности

Члан 33.

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, Шеф Одељења за општу управу и послове органа општине је дужан да обавести начелника Општинске управе, како би он могао да приступи измени овог правилника, у циљу унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

II. Провера ИКТ система

Члан 34.

Проверу ИКТ система врши Одељење за општу управу и послове органа општине.

Провера ће се вршити последњег месеца у години.

Провера се врши тако што се:

1) проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на која се врши упућивање, са прописаним условима, односно проверава да ли су правилником 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, 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 начелнику Општинске управе.

III. Садржај извештаја о провери ИКТ система

Члан 35.

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава;

2) време провере;

3) подаци 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.

IV. Прелазне и завршне одредбе

Члан 36.

Овај правилник ступа на снагу даном доношења и биће објављен у „Службеном гласнику општине Деспотовац“.

Члан 37.

Ступањем на снагу овог Правилника престаје да важи Правилник о безбедности информационо-комуникационог система Општинске управе Деспотовац бр. 110-5/2017-04 од 10.02.2017. године.

ОПШТИНСКА УПРАВА ДЕСПОТОВАЦ
Број: 110-4/2019-04 од 04.12.2019. године

НАЧЕЛНИК
ОПШТИНСКЕ УПРАВЕ
Гордана Јаблановић, дипл.правник с.р.

С А Д Р Ж А Ј

Оснивач:

Скупштина општине Деспотовац

Уредник:

Дамјан Крстовић, дипл.правник
Секретар Скупштине општине Деспотовац

Издаје и штампа:

Општинска управа Деспотовац
ул. Милосава Здравковића Ресавца бр. 4

Тел/факс:

(035) 611-006

Email:

sodespotovac@ptt.rs

Web:

www.despotovac.rs

2020

Д е с п о т о в а ц