

СЛУЖБЕНИ ЛИСТ

ГРАДА ЛОЗНИЦЕ



Година ХЛІ • Број 19
29. децембар 2017. године • Лозница

- ГРАДСКО ВЕЋЕ -

1

На основу члана 58. Закона о запосленима у аутономној покрајини и јединицама локалне самоуправе („Службени гласник РС” број 21/2016), и члана 25. став 1. тачка 2. Одлуке о Градској управи града Лозница („Службени лист града Лознице” број 19/16,25/16 и 13/17”), Одлуке о утврђивању максималног броја запослених на неодређено време у организационим облицима у систему јавног сектора града Лознице за 2017. годину („Службени лист града Лознице” број 13/17”), и сагласности Синдикалне организације самосталног синдиката синдикалне организације Градске управе града Лозница од 12.12.2017. године Градско веће града Лознице на предлог начелника Градске управе града Лознице, дана 28.12.2017. године, усвојило је

ПРАВИЛНИК О ИЗМЕНАМА И ДОПУНАМА ПРАВИЛНИКА О ОРГАНИЗАЦИЈИ И СИСТЕМАТИЗАЦИЈИ РАДНИХ МЕСТА У ГРАДСКОЈ УПРАВИ, ГРАДСКОМ ПРАВОБРАНИЛАШТВУ, СТРУЧНИМ СЛУЖБАМА И ПОСЕБНИМ ОРГАНИЗАЦИЈАМА ГРАДА ЛОЗНИЦА

Члан 1.

У Правилнику о организацији и систематизацији радних места у Градској управи, Градском правобранилаштву и посебним организацијама града Лозница, број: 06-35-1/17-II од 29.11.2017. године.

У ПОГЛАВЉУ I ОДЕЉЕЊЕ ЗА ПРИВРЕДУ И ЛОКАЛНИ ЕКОНОМСКИ РАЗВОЈ- Одсек за комуналну привреду, КОД РАДНОГ МЕСТА ПОД:

- редним бројем „2“ – „ЕКОНОМСКИ ПОСЛОВИ У ОБЛАСТИ КОМУНАЛНИХ ДЕЛАТНОСТИ“

Број службеника: „1“ замењује се бројем „2“.

Члан 2.

У ПОГЛАВЉУ III ОДЕЉЕЊЕ ЗА ПЛАНИРАЊЕ И ИЗГРАДЊУ- Одсек за спровођење обједињене процедуре и планирања, РАДНО МЕСТО ПОД:

Радним бројем „5” - „ Регистратор регистра обједињених процедура” се брише



Радно место под редним бројем: „6” - „Администратор за послове обједињене процедуре”, постаје радно место под редним бројем „5”.

Члан 3.

У ПОГЛАВЉУ V ОДЕЉЕЊЕ ЗА ОПШТУ УПРАВУ- Одсек за послове правне помоћи и писарнице, КОД РАДНОГ МЕСТА ПОД:

- редним бројем „6”- „СТРУЧНИ ПОСЛОВИ АРХИВСКОГ И КАНЦЕЛАРИЈСКОГ ПОСЛОВАЊА”

Број службеника: „1” замењује се бројем „2”.

Члан 4.

У ПОГЛАВЉУ V ОДЕЉЕЊЕ ЗА ОПШТУ УПРАВУ- Одсек за матичне послове и месне канцеларије, КОД РАДНИХ МЕСТА ПОД:

- редним бројем „5” - „ШЕФ МЕСНЕ КАНЦЕЛАРИЈЕ - МАТИЧАР”

Број службеника: „6” замењује се бројем „5”.

- редним бројем „7” - „ ЗАМЕНИК ШЕФА МЕСНЕ КАНЦЕЛАРИЈЕ – ЗАМЕНИК МАТИЧАРА”

Број службеника: „11” замењује се бројем „9”.

Члан 5.

У ПОГЛАВЉУ VI ОДЕЉЕЊЕ ЗА ДРУШТВЕНЕ ДЕЛАТНОСТИ- Одсек за јавне службе, отвара се ново радно место под редним бројем „6”.

6. ПОСЛОВИ НАДЗОРА И КОНТРОЛЕ СПОРТСКИХ КЛУБОВА И УДРУЖЕЊА

Опис послова:

Врши контролу утрошених средстава по пројектима који су удружењима одобрени од стране града Лознице. Обавља послове стручне обраде подентих захтева и правдања средстава одобрених спортским клубовима, удружењима из области културе, медија, верских заједница као и удружењима грађана из области социјалне заштите. Води службене регистре све неопходне евиденције везано за трошење буџетских средстава од стране спортских клубова, удружења из области културе, медија, верских заједница као и удружења грађана из области



социјалне заштите и израђује извештаје о истом у наведеним областима. Прати и примењује законске прописе из наведених области. Непосредно комуницира са представницима спортских клубова и удружења, сарађује са министарствима и другим државним органима по питањима која се односе на спортске клубове и удружења.

Обавља и друге послове по налогу начелника и помоћника начелника одељења. За свој рад непосредно је одговоран шефу одсека и начелнику одељења.

Стручна спрема: Високо образовање стечено на студијама другог степена из области економских наука у обиму од најмање 240 ЕСПБ бодова (дипломске академске студије, специјалистичке академске студије специјалистичке струковне студије), односно дипломирани економиста са стеченим образовањем на основним студијама у трајању од најмање четири године.

Звање: Млађи саветник

Додатно знање/испити: Положен државни стручни испит за рад у органима државне управе.

Радно искуство: Најмање једна година радног искуства у струци.

Посебни услови: Познавање рада на рачунару (MS Office пакет и интернет).

Број службеника: 1

Члан 6.

У ПОГЛАВЉУ VII ОДЕЉЕЊЕ ЗА РАД ОРГАНА, ИНФОРМАЦИОНЕ И ЗАЈЕДНИЧКЕ ПОСЛОВЕ - Одсек за информационе технологије (ИТ), КОД РАДНОГ МЕСТА ПОД:

- редним бројем „4” - „ПОСЛОВИ ЗА ИТ АДМИНИСТРАЦИЈУ И ОДРЖАВАЊЕ МРЕЖЕ ”

Број службеника: „1” замењује се бројем „2”.

Члан 7.

Овај Правилник ступа на снагу даном усвајања, односно доношења и биће објављен у „Службеном листу града Лознице”.

Број: 06-42-1/17- II

Дана 28.12.2017. године

Л о з н и ц а

ГРАДОНАЧЕЛНИК
ПРЕДСЕДНИК
ГРАДСКОГ ВЕЋА
Видоје Петровић,с.р.



- ГРАДСКА УПРАВА -

2

На основу члана 8. Закона о информационој безбедности („Службени гласник РС”, број 6/16), 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) и члана 3. Одлуке о Градској управи града Лознице („Сл. лист града Лознице”, бр. 19/16, 25/16 и 13/17), начелник Градске управе дана 28. децембра 2017. године, донео је

П Р А В И Л Н И К

о безбедности информационо - комуникационог система града Лознице

I. Уводне одредбе

Члан 1.

Овим Правилником утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система града Лознице (у даљем тексту: ИКТ систем), у складу са Законом о информационој безбедности и подзаконским актима.

Члан 2.

Мере прописане овим Правилником се односе на све организационе јединице Градске управе града Лознице на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе града Лознице.

Непоштовање одредби овог Правилника повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса града Лознице.

За праћење примене овог Правилника обавезује се Одсек за информационе технологије (у даљем тексту: Одсек за ИТ).

Члан 3.

Поједини термини у смислу овог Правилника имају следеће значење:

- 1) *информационо-комуникациони систем* (ИКТ систем) је технолошко-организациона целина која обухвата:
 - (1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
 - (2) 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;



- (3) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- (4) организациону структуру путем које се управља ИКТ системом;
- 2) *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;
- 3) *тајност* је својство које значи да податак није доступан неовлашћеним лицима;
- 4) *интегритет* значи очуваност изворног садржаја и комплетности податка;
- 5) *расположивост* је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
- 6) *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;
- 7) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
- 8) *ризик* значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
- 9) *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;
- 10) *инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
- 11) *мере заштите ИКТ система* су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
- 12) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
- 13) *ИКТ систем за рад са тајним подацима* је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
- 14) *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
- 15) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
- 16) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
- 17) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;
- 18) *криptomатеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
- 19) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
- 20) *информациона добра* обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;



- 21) VPN (Virtual Private Network)-je „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;
- 22) MAC адреса (Media Access Control Address) је јединствен број, којим се врши идентификација уређаја на мрежи;
- 23) Backup је резервна копија података;
- 24) Download је трансфер података са централног рачунара или web презентације на локални рачунар;
- 25) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
- 26) Freeware је бесплатан софтвер;
- 27) Opensource софтвер отвореног кода;
- 28) 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;
- 29) USB или флеш меморија је спољшњи медијум за складиштење података;
- 30) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;
- 31) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

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 града Лознице

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 града Лознице надлежан је Одсек за ИТ.

Члан 6.

Под пословима из области безбедности утврђују се:

- 1) послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност,



- 2) послови управљање ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности,
- 3) послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система града, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе,
- 4) праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу,
- 5) обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента Одсек за ИТ, обавештава начелника Градске управе, који у складу са прописима обавештава надлежне органе у циљу решавања насталог безбедоносног инцидента.

2. Безбедност рада на даљину и употреба мобилних уређаја

Члан 7.

Нерегистровани корисници, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ Интернету али не и деловима мреже кроз коју се обавља службена комуникација.

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву Града/Општине/Градске општине, и који су подешени од стране Одсека за ИТ, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности, а на основу писане сагласности начелника Управе.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и листе MAC адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Приступ ресурсима ИКТ система града Лознице са удаљених локација, од стране запослених-корисника, у циљу обављања радних задатака, омогућен је путем заштићене VPN/интернет конекције.

Запосленом-кориснику, забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.)

Одсек за ИТ, свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан обавештава начелник Градске управе, а та MAC адреса се уноси у „block“ листу софтвера који се користи за контролу приступа.

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

Евиденцију приватних уређаја са којих ће бити омогућен приступ води Одсек за ИТ, а по одобрењу начелника Управе.

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране Одсека за ИТ, могу се користити само за обављање послова у надлежности



корисника-запосленог и то само у периоду када није могуће користити уређај у власништву града Лознице.

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

Члан 8.

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

Одсек за ИТ је дужан да сваког новозапосленог-корисника ИКТ ресурса упозна са одговорностима и правилима коришћења ИКТ ресурса града Лознице, да га упозна са правилима коришћења ресурса ИКТ система, као и да води евиденцију о изјавама новозапослених – корисника да су упознати са правилима коришћења ИКТ ресурса.

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

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

Члан 9.

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

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

О престанку радног односа или радног ангажовања, као и промени радног места, Група за управљање људским ресурсима, у сарадњи са непосредним руководиоцем, је дужна да обавести Одсек за ИТ, ради укидања, односно измену приступних привилегија тог запосленог-корисника.

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

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра града Лознице су сви ресурси који садрже пословне информације Градске управе града Лознице, 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 рад органа града, информационе и заједничке послове, у папирној или електронској форми, преко Одеска за ИТ и Службе за одржавање зграде.

Предмет заштите су:

- 1) хардверске и софтверске компоненте ИКТ система,
- 2) подаци који се обрађују или чувају на компонентама ИКТ система,
- 3) 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.

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

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).

7. Заштита носача података

Члан 12.

Одсек за ИТ 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.

Евиденцију носача на којима су снимљени подаци, воде надлежна Одељења Градске управе 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 Градске 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 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 Града 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;
- 9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
- 10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
- 11) израђује заштитне копије (backup) података у складу са прописаним процедурама;
- 12) користи интернет и електронску пошту у складу са прописаним процедурама;
- 13) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
- 14) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
- 15) 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;
- 16) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.



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

Члан 14.

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

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

Администраторски налог могу да користе само запослени на пословима: шефа Одсека, администратора ИТ система, за веб информатички развој и за ИТ администрацију и одржавање мреже.

Администраторски налог за управљање доменом може да користи само запослени на пословима администратора ИТ система.

Администраторски налог за управљање базом података може да користи само запослени на пословима администратора ИТ система, за веб информатички развој и за ИТ администрацију и одржавање мреже.

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

Кориснички налог додељује администратор, на основу захтева непосредног руководиоца, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу налога надлежног руководиоца.

10. *Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију*

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке.

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

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 16.

За приступ ресурсима ИКТ система који се односе на послове одбране, односно, за које је надлежно министарство прописало коришћење криптозаштите, посебним



правилником ће бити дефинисана употреба одговарајућих мера криптозаштите узимајући у обзир осетљивост информација које треба да се штите, пословне процесе који се спроводе, ниво захтеване заштите, имплементацију примењених криптографских техника и управљање криптографским кључевима.

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.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује се 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 мора да буде обезбеђен од компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор).

О уласку у ову зону води се посебна евиденција.

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, односно административној зони, дозвољен је само начелнику Одељења за рад органа града, информационе и заједничке послове, шефу Одсека за информационе технологије, шефу Службе за одржавање зграде и администратору ИКТ система.

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 Градске управе, и уз присуство лица коме је дозвољен улаз.

Приступ административној зони може имати и запослени на пословима одржавања хигијене уз присуство надлежног лица, односно шефа Службе за одржавање зграде.

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.

Прозори и врата на овој просторији морају увек бити затворени.



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 неопходно је одобрење начелника Градске управе који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења начелника Градске 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 града.

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 Градске 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 приметне битне 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, аутоматски се врши допуна антивирусних дефиниција.

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 града са интернета, Одсек за ИТ је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему Одсек за ИТ 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 Одсек за ИТ.

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 Одсеку за ИТ.

Строго је забрањено гледање филмова, играње игрица на рачунарима и прегледање WEB страница 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 нелегалних 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 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.

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

Члан 21.

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



Систем за контролу и дојаву о грешкама, неовлашћеним активностима и др, мора бити подешен тако да одмах обавештава администратора, шефа Одсека за ИТ и начелника Градске управе, о свим нерегуларним активностима запослених-корисника, покушајима упада и упадима у систем.

17. Обезбеђивање интегритета софтвера и оперативних система

Члан 22.

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

Инсталацију и подешавање софтвера може да врши Одсек за ИТ, 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.

18. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 23.

Одсек за ИТ 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, Одсек за ИТ је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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

Члан 24.

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 Градске управе.

20. Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 25.

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 гаск орману.

Одсек за ИТ 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 Градске управе, мора бити одвојена од интерне мреже коју користе корисници запослени у Управи и кроз коју се врши размена службених података.

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

Члан 26.

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

Одсек за ИТ је задужен и 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 Одсек за ИТ води документацију.

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

Члан 27.

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

Приликом тестирања система, подаци који су означени ознаком тајности, односно службености као поверљиви подаци, или су лични подаци Одсек за ИТ, одговара за податке у складу са прописима којима је дефинисана употреба и заштита такве врсте података).

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

Члан 28.

Трећа лица-пужаоци 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.

Одсек за ИТ је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог Правилника којима су такве активности дефинисане.



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

Члан 29.

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

По пријему пријаве Одсек за ИТ је дужан да одмах обавести начелника Одељења 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 инцидента и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, „Сл. Гласник РС“, бр, 94/2016), Одсек за ИТ је дужан да поред начелника обавести и надлежни орган дефинисан овом уредбом.

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

25. Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 30.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде Градске управе, Одсек за ИТ, је дужан да у најкраћем року пренесе делове ИКТ система (или обезбеди функционисање редувантних компоненти на резервној локацији уколико постоје) 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 Одсек за ИТ, и то у три примерка, од којих се један налази код Одсека, други код запосленог надлежног за послове одбране и ванредне ситуације а трећи примерак код начелника Градске управе.

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

III. Измена Правилника о безбедности

Члан 31.

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, Одсек за ИТ је дужан да обавести



начелника Градске управе, како би он могао да приступи измени овог Правилника, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

IV. Провера ИКТ система

Члан 32.

Проверу ИКТ система врши Одсек за ИТ.

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 дали 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 Градске управе.

V. Садржај извештаја о провери ИКТ система

Члан 33.

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.



VI. Прелазне и завршне одредбе

Члан 34.

Овај Правилник ступа на снагу даном доношења и биће објављен у “Службеном листу града Лознице”.

Број: 110-1/2017-III,
Датум: 28.12.2017. године
Лозница

НАЧЕЛНИК
ГРАДСКЕ УПРАВЕ
Милојка Смиљанић, дипл. правник, с.р.

3

На основу члана 25. Одлуке о градској управи града Лознице („Службени лист града Лознице“, број 19/16, 25/16 и 13/17), доносим следећи

П Р А В И Л Н И К О ПРОТОКОЛАНРИМ И ПРИГОДНИМ ПОКЛОНИМА

I ОПШТЕ ОДРЕДБЕ

Члан 1.

Правилником о поклонима са протоколарном наменом (у даљем тексту: Правилник) уређују се услови давања и примања поклона које у вези са вршењем функције даје и прима функционер, службеник на положају и друго запослено лице, начин располагања примљеним поклонима као и начин евиденције примљених и датих поклона.

Члан 2.

Под поклоном се у смислу овог Правилника сматрају протоколарни и пригодни поклони чија вредност не прелази 5% просечне месечне зараде у Републици Србији.

Протоколарни поклон је поклон који овлашћено лице даје међународном и домаћем органу или организацији, домаћем или страном правном лицу односно њиховим представницима приликом пријема, службене посете, гостовања или другим сличним околностима, као и онај који у овим ситуацијама овлашћено лице прима.



Пригодни поклони се уручују у приликама када људи традиционално размењују дарове.

Легитимациони папири, као што су карте и улазнице за културне, спортске и сличне манифестације, нису поклони по овом правилнику, уколико на њима пише да су бесплатни примерци, односно да су у облику позивнице.

Члан 3.

Вредност поклона је тржишна цена поклона, на дан када је поклон понуђен, односно примљен.

Тржишна цена поклона је просечна цена тог производа или услуге на локалном тржишту, односно просечна цена производа или услуге сличне врсте и вредности у слободној продаји на тржишту.

Члан 4.

Протоколарни поклони и пригодни поклони за које се након уручења утврди да прелазе вредност од 5% просечне месечне зараде без пореза и доприноса у Републици Србији, односно пригодни поклони чија укупна вредност прелази износ од једне просечне месечне зараде без пореза и доприноса у Републици Србији, постају јавна својина Града.

У протоколарне и пригодне поклоне, без обзира на њихову вредност, не рачунају се поклони:

- чије је уручење или пријем забрањено законским прописима,
- ако су уручени у облику новца, хартија од вредности,
- ако би њихов пријем био у супротности са етичким стандардима који важе за одређене функционере.

Поклони из претходног става не могу постати власништво функционера и службеника на положају, нити јавна својина и потребно их је одбити, вратити поклонодавцу, односно треба са њима поступати у складу са законском регулативом.

Забрана и ограничења из овог члана односе се и на случајеве када се поклон у вези са вршењем јавне функције функционера и службеника на положају уручује повезаним лицима функционера и службеника на положају.

Члан 5.

Овлашћена лица из члана 2. овог Правилника су:

- градоначелник, заменик градоначелника;
- председник и заменик председника Скупштине града;
- секретар и заменик секретара Скупштине града;
- чланови Градског већа и помоћници градоначелника;
- начелници градских управа;
- и остала именована, изабрана и постављена лица.



II ПОСТУПАЊЕ У СЛУЧАЈУ ПРИМАЊА ПОКЛОНА

Члан 6.

Овлашћено лице који прими поклон дужно је да га одмах преда органу у коме врши јавну функцију односно где је запослено, са основним подацима о поклону у виду обавештења (Прилог 1. овог Правилника).

III ЕВИДЕНЦИЈА ДАТИХ И ПРИМЉЕНИХ ПОКЛОНА

Члан 7.

Евиденција поклона представља јединствену листу примљених поклона, сачињену на основу поднетих обавештења о примљеним поклонима, означену редним бројем, према хронолошком редоследу примања.

Евиденција садржи: назив органа у којој овлашћено лице врши јавну функцију односно је запослено, име и презиме овлашћеног лица, функцију коју врши, име, презиме и адресу поклонодавца, односно име и седиште правног лица или органа, уколико је поклон дат у име правног лица или органа, датум пријема поклона, податак да ли се ради о протоколарном или пригодном поклону, опис поклона, место и датум попуњавања евиденције, потпис примаоца поклона.

Евиденција поклона води се за временски период календарске године.

Свако овлашћено лице има право на увид у евиденцију поклона у вези са подацима који се односе на исти.

Члан 8.

За вођење евиденције датих и примљених поклона задужена је Градска управа надлежна за послове градоначелника.

Град је дужан да до 1. марта текуће године, евиденцију примљених поклона за претходну годину достави Агенцији за борбу против корупције у електронској форми - приступом апликацији на веб сајту Агенције и у штампаној форми-непосредно, препорученом поштанском пошиљком, одмах а најкасније у року од осам дана по добијању програмски генерисане шифре којом се потврђује електронска регистрација евиденције поклона.

На основу прикупљених примерака евиденције, Агенција за борбу против корупције израђује каталог примљених поклона за претходну календарску годину и објављује га на свом сајту до 1. јуна текуће године.

Примљени поклони чувају се у згради Градске управе града Лознице.

Члан 9.

Евиденција датих поклона води се на основу потврде (Прилог 2. овог Правилника) о издатим поклонима, коју издаје лице запослено у Градској управи надлежној за послове градоначелника, које ради на пословима из области протокола.



IV ДАВАЊЕ И НАБАВКА ПРОТОКОЛАРНИХ ПОКЛОНА

Члан 10.

Право на давање протоколарних поклона имају овлашћена лица из члана 5. овог Правилника.

Право на давање поклона могу имати и остала запослена лица на основу писаног одобрења неког од овлашћених лица.

Члан 11.

Градска управа надлежна за послове градоначелника планира и врши набавку протоколарних и пригодних поклона у складу са висином одобрених средстава у буџету Града за текућу годину.

V НАДЗОР НАД СПРОВОЂЕЊЕМ ОДРЕДБИ ПРАВИЛНИКА

Члан 12.

Унутрашњу контролу спровођења одредби овог правилника спроводи начелник Управе надлежне за послове градоначелника. За унутрашњу контролу начелник може да овласти и друго лице.

Спољну контролу спровођења одредби овог Правилника спроводи Агенција за борбу против корупције у складу са овлашћењима која су утврђена Законом о Агенцији за борбу против корупције.

VI ЗАВРШНЕ ОДРЕДБЕ

Члан 13.

Овај Правилник ступа на снагу даном објављивања у “Службеном листу града Лознице”.

Број: 110-2/2017-III,

Датум: 28.12.2017. године

Л о з н и ц а

**НАЧЕЛНИК
ГРАДСКЕ УПРАВЕ
Милојка Смиљанић, дипл.правник, с.р.**

**Прилог 1.****ОБАВЕШТЕЊЕ О ПРИМЉЕНОМ ПОКЛОНУ**

У складу са Правилником о протоколарним и пригодним поклонима, подноси се обавештење о примљеном поклону.

1. Подаци о функционеру	
1.1. Име, презиме и функција функционера односно службеника на положају:	
2. Подаци о примљеном поклону	
2.1. Поклонодавац (име и презиме или назив и седиште органа ако је поклон дат у име правног лица или тела, датум пријема, уколико је поклон примљен поштом или на други посредан начин навести ту чињеницу и навести податке који су приликом пријема поклона познати):	
2.2. Поклон:	а) протоколаран б) пригодан
2.3. Повод за уручење поклона:	
2.4. Опис поклона	

У Лозници, _____ . године

(ПОТПИС)



Прилог 2.



Република Србија
 ГРАД ЛОЗНИЦА
 ГРАДСКА УПРАВА
 Број:
 Дана:
 Л о з н и ц а

ПОТВРДА О ИЗДАТИМ ПОКЛОНИМА

На основу захтева _____, _____, у
 (име и презиме) (функција)
 оквиру реализације службеног пута и посете _____,
 (место и земља која се посећује или која гостује)

издаје се поклон следеће садржине:

- _____
 - _____

Поклон примио,

Поклон издао,

САДРЖАЈ

Број	Назив акта	Страна
------	------------	--------

- ГРАДСКО ВЕЋЕ -

- ПРАВИЛНИК О ИЗМЕНАМА И ДОПУНАМА ПРАВИЛНИКА О ОРГАНИЗАЦИЈИ И СИСТЕМАТИЗАЦИЈИ РАДНИХ МЕСТА У ГРАДСКОЈ УПРАВИ, ГРАДСКОМ ПРАВОБРАНИЛАШТВУ, СТРУЧНИМ СЛУЖБАМА И ПОСЕБНИМ ОРГАНИЗАЦИЈАМА ГРАДА ЛОЗНИЦА 1

- ГРАДСКА УПРАВА -

- ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНОГ СИСТЕМА ГРАДА ЛОЗНИЦЕ 4
- ПРАВИЛНИК О ПРОТОКОЛАНРИМ И ПРИГОДНИМ ПОКЛОНИМА 19