На основу члана 8.став 1. Закона о информационој безбедности („Службени гласник РС", број 6/16), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо–комуникационих система од посебног значаја („Службени Гласник РС", број 94/16) и члана 35. став 1. тачка3. у вези са чланом 50. став 2. Одлуке о Градској управи града Краљева („Службени лист града Краљева", број 35/16),

Начелник Градске управе града Краљева,дана 13.02.2024.године, донео је

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ГРАДСКЕ УПРАВЕ ГРАДА КРАЉЕВА

ОСНОВНЕ ОДРЕДБЕ

Опште одредбе

Члан 1.

Правилником о безбедности информационо-комуникационог система, у складу са Законом о информационој безбедности („Службени гласник РС", број 6/16, у даљем тексту:Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности увези са безбедношћу и ресурсима информационо-комуникационог система (у даљем тексту: ИКТ систем).

Циљеви Правилника о безбедности ИКТ система

Члан 2.

ЦиљевиДоношењаПравилника о безбедности ИКТ система су:

1) одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2) спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
3) подизање свести код запослених о значају информационе безбедности,ризицима и мерама заштите приликом коришћења ИКТ система;
4) прописивање овлашћења и одговорности запослених у вези са безбедношћу иресурсима ИКТ система;
5) свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Правилника о безбедности ИКТ система

Члан 3.

Мере заштите ИКТ система које су ближе уређене Правилником о безбедности ИКТ система служе превенцији од настанка инцидената и умањењу штете од инцидената и њихова примена је обавезна за све запослене. Запослени морају бити упознати са садржином Правилником о безбедности ИКТ

система и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

Одговорност запослених

Члан 4.

Запослени су дужни да приступају информацијама и ресурсима ИКТ система само радио бављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

Предмет заштите

Члан 5.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге,техничку и корисничку документацију, унутрашње опште акте и процедуре.

I. МЕРЕ ЗАШТИТЕ

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

Члан 6.

Организациона структура представља скуп задатака и овлашћења којим се уређује начин на који запослени обављају своје активности и користе расположиве ресурсе за постизање циљева организације.

Одељење информационих технологија је задужено и одговорно за управљање информационом безбедношћу ИКТ система.

Администратор за безбедност информационих система и технологија је задужен да:

- Прати примене које могу утицати на опште стање заштите информација ;
- Прати и анализира сигурносне инциденте;
- додељује улоге у поступку заштите;
- координира и контролише примену мера заштите;
- обавештава надлежне државне органе о инцидентима у ИКТ систему, усклади са прописима.

Члан 7.

Оператор ИКТ система (Градска управа града Краљева) 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.

Заштита од ризика који настају при променама послова или престанка радногангажовања запослених лица

Члан 8.

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.

За поступања приликом престанка запослења или ангажовања администратор за безбедност информационих система и технологија је задужен је да предузима следеће активности :

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату;
- прегледа све налоге и приступе систему који су били доступни запосленом;
- преузима од запосленог електронске и друге уређаје;
- проверава враћене уређаје и уређаје за преношење података;
- укида налоге електронске поште на дан престанка радног односа или другог основа ангажовања бившег запосленог;
- прегледа све налоге за приступ одлазећег запосленог и прикупља приступне шифре и кодове са циљем укидања/промене истих на дан одласка;

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 9.

Информациона добра обухватају податке у датотекама и базама података, програмски код, хардверске компоненте, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности

Члан 10.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоатајности податка, у складу са њиховим значајем.

Заштита носача података

Члан 11.

Одељење информационих технологија обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података.

Ограничење приступа подацима и средствима за обраду података

Члан 12.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности података. Корисницима се додељују минимална права приступа и привилегије за приступ ИКТ добрима потребна за обављање пословних задатака, укључујући у то и приступ рачунарској мрежи и мрежним ресурсима.

Ограничење приступа подразумева:

• физичку контролу приступа (браве);

• административно ограничење приступа (раздвајање надлежности);

• техничка контрола приступа (корисници система са дефинисаним врстама приступа у оквиру мрежних уређаја, логови догађаја у систему, софтвер за заштиту од злонамерног софтвера, бекап података и слично).

Ограничење приступа врши се у складу са улогом корисника ИКТ система. Све методе контроле приступа морају се разматрати заједно. Приступ се ограничава уређајима које корисник користи за приступ информационим и техничким ресурсима. Контрола минимално подразумева аутентикацију корисника и контролу приступа информационим услугама.

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

Члан 13.

Одељење информационих технологија управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 14.

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

Сви корисници су дужни да:

• корисничко име и шифру држе у тајности, не откривају их другим лицима,укључујући и надређене особе;

• избегавају чување корисничког имена и шифре у писаном облику;

• промене шифру када примете да постоји било какав наговештај могућег компромитовања.

Шифре морају да:

• Садрже најмање 6 алфанумеричких карактера;

• Садрже најмање једну цифру.

Корисници су дужни да привремене шифре промене приликом првог пријављивања.

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

Члан 15.

У циљу заштите података Одељење информационих технологија развија и имплементира политику коришћења криптографских контрола, и успоставља механизме и систем зауправљање кључевима.

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

Члан 16.

Одељење информационих технологија је дужно да предузме мере ради спречавања неовлашћеног физичког приступа објекту, простору, просторијама, зони, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација и опреме за обраду информација. Измештање имовине ИКТ система може да се врши само уз претходно одобрење овлашћеног лица, уз примену безбедносних механизама, узимајући у обзир различите ризике приликом рада изван просторија организације.

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

Члан 17.

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасностииз окружења, као и могућности за неовлашћени приступ.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 18.

Одељење информационих технологија спроводи радне процедуре које обезбеђују исправно и безбедно извршење следећих послова:

а) инсталација и конфигурација система;

б) обраду и поступање са информацијама (аутоматски и мануелно);

в) израда резервних копија;

г) захтеви за временски распоред активности;

д) инструкције за поступање према грешкама или другим ванредним стањима која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција;

ђ) контакти за подршку (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;

е) инструкције за поступања према поверљивим подацима;

ж) процедуре за поновно покретање система и опоравак, које се користе у случајуотказа система;

з) управљање информацијама о трагу провере система и системским записима(логовима);

и) процедуре за надгледање.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 19.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежајурад или оштете податке и/или рачунар. Заштита од злонамерног софтвера се заснива на софтверу за откривање злонамерног софтвера и отклањање штете, на познавању безбедности информација, као и на одговарајућим контролама приступа систему и управљања захтеваним и потребним променама.

Заштита од губитка података

Члан 20.

Одељење информационих технологија врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима. Резервне копије података се раде на дневном,недељеном и месечном нивоу. Резервне копија остајена серверу, а као додатна мера копирају се на хард диск намењен прављењу резервних копија или се нарезује на двд дискове. За копирање података задужен је администратор за безбедност информационих система и технологија или неко друго лице запослено у одељењу информационих технологија.

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

Члан 21.

У ИКТ систему формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Обезбеђивање интегритета софтвера и оперативних система

Члан 22.

Одељење информационих технологија спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 23.

Одељење информационих технологија врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

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

Члан 24.

Приликом спровођења ревизије ИКТ система Одељење информационих технологија обезбеђује да ревизија има што мањи утицај на функционисање система.

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

Члан 25.

Заштита података који се преносе комуникационим средствима обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

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

Члан 26.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, Одељење информационих технологија је у обавези даобезбеди безбедност информација у свакој фази. Питање безбедности се

анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења.

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

Члан 27.

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

Заштита средстава оператора ИКТ система која су доступна пружаоцимауслуга

Члан 28.

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

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

Члан 29.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности ипружених услуга у складу са условима који су уговорени са пружаоцем услуга, Одељење информационх технологија успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

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

Члан 30.

Посебним процедурама се уређује начин одговора на инциденте нарушавања безбедности информација и одређује особа за контакт у случајевима нарушавања безбедности, као и контакте са овлашћеним телима.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 31.

Одељење информационих технологија примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

Измена Правилника

Члан 32.

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, Одељење информационих технологија је дужно 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 преиспитивања овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Прелазне и завршне одредбе

Члан 33.

Доношењем овог Правилника престаје да важи Правилник о информационом систему Градске управе града Краљева („Службени лист града Краљева“,број 5/2017).

Члан 34.

Овај Правилник ступа на снагу осмог дана од дана објављивања у „Службеном листу града Краљева“.

ГРАДСКА УПРАВА ГРАДА КРАЉЕВА
Број:372/ 2024.године

НАЧЕЛНИК ГРАДСКЕ УПРАВЕ
Дејан Ћајић, дипл. правник