На основу члана 8. Закона о информационој безбедности („Сл. гласник РС“, бр. 6/2016, 94/2017 и 77/2019), Уредбе о ближем садржају аката о безбедности ИКТ система („Сл. гласник РС“, бр. 12/2020) и члана 49. став 1. и став 2. алинеја пета Статута Стамбене агенције Града Новог Сада, директор Стамбене агенције Града Новог Сада, доноси:

ПРАВИЛНИК О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ И ЗАШТИЦИ ИКТ СИСТЕМА У СТАМБЕНОЈ АГЕНЦИЈИ ГРАДА НОВОГ САДА

I ОСНОВНЕ ОДРЕДБЕ

Члан 1. (Предмет Правилника)

Овим правилником уређују се мере, обавезе, одговорности, технички и организациони стандарди за заштиту информационо-комуникационог система (у даљем тексту: ИКТ систем), рачунарске мреже, базе података, софтверских апликација, хардвера и информационе имовине у Стамбеној агенцији Града Новог Сада (у даљем тексту: Агенција).

Члан 2. (Сврха и циљеви)

Основу информационе безбедности чини очување три кључна принципа:

1. **Поверљивост (Confidentiality):** Обезбеђивање да подаци и информације буду доступни искључиво овлашћеним лицима;
2. **Интигритет (Integrity):** Заштита тачности, потпуности и изворности информација и метода обраде;
3. **Расположивост (Availability):** Обезбеђивање да овлашћени корисници имају правовремени приступ подацима и ИКТ ресурсима када су им потребни за обављање послова.

Члан 3. (Примена)

Одредбе овог правилника односе се на све запослене у Агенцији, као и на екстерне сараднике, даваоце ИТ услуга и трећа лица која по било ком основу имају овлашћен приступ ИКТ систему Агенције.

II УПРАВЉАЊЕ И ИМЕНОВАЊЕ ОДГОВОРНИХ ЛИЦА

Члан 4. (Администратор ИКТ система)

Директор Агенције одређује **Лице одговорно за безбедност ИКТ система (Администратор ИКТ система)** из реда запослених стручних лица или путем уговора о ангажовању стручног правног лица/екстерног оператера.

Администратор ИКТ система одговоран је за спровођење мера заштите, праћење рада мреже, управљање корисничким налозима, израду резервних копија (backup) и реакцију на безбедносне инциденте.

III КОРИШЋЕЊЕ РАЧУНАРСКЕ ОПРЕМЕ И РЕСУРСА

Члан 5. (Лозинке и кориснички налози)

1. Сваком запосленом додељује се јединствени кориснички налог и почетна лозинка за приступ рачунару и мрежним ресурсима.
2. Запослени су дужни да корисничке лозинке држе у тајности. Забрањено је записивање лозинки на видним местима (нпр. на монитору, тастатури или радном столу) или њихово дељење са колегама.
3. Лозинке морају бити сложене (минимално 8 карактера, комбинација великих и малих слова, бројева и специјалних знакова) и морају се мењати у дефинисаним временским интервалима (најмање једном у 90 дана).
4. Након истека радног времена или приликом привременог напуштања радног места, запослени је дужан да закључа свој рачунар (комбинацијом тастера Win + L или одјавом са система).

Члан 6. (Коришћење имејла и интернета)

1. Службена имејл адреса и интернет приступ користе се искључиво у пословне сврхе.
2. Забрањено је отварање имејл порука, прилога или линкова добијених од непознатих, сумњивих или непроверених пошилаца ради спречавања продора малиционог софтвера (вируса, *ransomware*-а, *phishing*-а).
3. Забрањено је преузимање (download) незаконитог садржаја, инсталација нелиценцираног софтвера, као и коришћење *peer-to-peer* сервиса на рачунарима Агенције.

Члан 7. (Екстерни медији и мобилни уређаји)

1. Забрањено је прикључивање приватних USB меморија, екстерних хард дискова и других непознатих уређаја на рачунаре Агенције без претходне провере и одобрења Администратора IKT система.
2. Коришћење приватних уређаја (мобилни телефони, лаптопови) у службене сврхе или нихово повезивање на интерну мрежу Агенције није дозвољено, осим путем посебно изоловане мреже за госте (Guest network).

IV ТЕХНИЧКЕ МЕРЕ ЗАШТИТЕ И БЕЗБЕДНОСТ ПОДАТАКА

Члан 8. (Антивирусна заштита и ажурирање)

1. Сви рачунари и сервери у Агенцији морају имати инсталиран и активан лиценцирани антивирус софтвер.
2. Администратор IKT система дужан је да обезбеди редовно ажурирање оперативних система, антивирусних база и апликативног софтвера најновијим безбедносним закрпама.

Члан 9. (Резервне копије - Backup)

1. Ради заштите од губитка података услед хардверских кварова, сајбер напада или људске грешке, Агенција врши редовно израђивање резервних копија свих битних база података, документације и електронске поште.
2. Резервне копије морају се сачињавати аутоматски на дневном, недељном и месечном нивоу.
3. Најмање једна копија података мора се чувати на локацији физички одвојеној од главног сервера (офф-сите или заштићени облак/cloud сервис), уз обавезну криптографску заштиту (енкрипцију).

Члан 10. (Физичка безбедност IKT опреме)

1. Серверска опрема, мрежни преклопници (switch) и централни комуникациони ормари морају бити смештени у посебној, закључаној просторији са контролисаним приступом.
2. У просторију са серверском опремом приступ имају искључиво овлашћена лица.
3. Физичке просторије морају бити заштићене од пожара, poplava, прекомерне топлоте и струјних удара (обезбеђивањем УПС уређаја за непрекидно напајање).

V ПОСТУПАЊЕ У СЛУЧАЈУ ИНЦИДЕНАТА И ОДГОВОРНОСТ

Члан 11. (Пријава безбедносног инцидента)

1. Запослени је дужан да одмах, без одлагања, пријави Администратору IKT система или непосредном руководиоцу сваку уочену неправилност, сумњу на вирус, губитак података, сумњив имејл или физичко оштећење опреме.
2. У случају сајбер напада или компромитовања система, Администратор IKT система предузима хитне мере изолације погођених уређаја са мреже и о томе обавештава директора и надлежни Национални ЦЕРТ / надлежно министарство у складу са Законом о информационој безбедности.

Члан 12. (Дисциплинска и материјална одговорност)

1. Непоштовање одредби овог правилника, неовлашћено одавање приступних параметара, намерно уношење малициоиог софтвера или ненаменско коришћење IKT ресурса представља тежу повреду радне дисциплине и радних обавеза.
2. Запослени који својом непажњом или намерним деловањем проузрокује штету на IKT систему подлеже дисциплинској, материјалној и кривичној одговорности у складу са законом.

VI ЗАВРШНЕ ОДРЕДБЕ

Члан 13.

Сви запослени дужни су да се упознају са одредбама овог правилника приликом ступања на рад или дан ступања овог правилника на снагу.

Члан 14.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли и интернет страници Стамбене агенције Града Новог Сада.

СТАМБЕНА АГЕНЦИЈА ГРАДА НОВОГ САДА

Број: 822-21 / 2026

Нови Сад, 4. 11. 2026. године

директор

Марко Јовановић

Доставити:

- Огласној табли
- Служби за правне и опште послове
- Служби за финансије и рачуноводство
- Архиви