На основу члана 10. и члана 12. Закона о информационој безбедности („Сл. гласник РС“, бр. 91/2025) и Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, Општина доноси

# Акт о безбедности ИКТ система — Општина

**ПОВЕРЉИВО — документ фирме „Општина“ садржи мере заштите и процедуре ИКТ система. Не дистрибуирати ван БДБ тима и овлашћених лица клијента.**

Датум генерисања: 08.11.2026. 03:32

Документ је припремљен на основу Анализе ризика, у складу са чл. 10 Закона о информационој безбедности („Сл. гласник РС“, бр. 91/2025) и Уредбом о ближем садржају акта о безбедности ИКТ система од посебног значаја. Пре усвајања од стране органа управљања, садржај проверити, допунити и уредити.

## Члан 1. Предмет акта

Овим актом о безбедности ИКТ система (у даљем тексту: Акт) одређују се мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система од посебног значаја Општина (у даљем тексту: ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

## Члан 2. Појмови и дефиниције

Поједини изрази употребљени у овом Акту имају следеће значење:

1) ИКТ систем је технолошко-организациона целина која обухвата електронске комуникационе мреже, уређаје или групе међусобно повезаних уређаја код којих се врши аутоматска обрада података, податке који се чувају, обрађују, претражују или преносе, организациону структуру и софтвер путем којих се тим системом управља;

2) информациона безбедност је способност ИКТ система и мрежа да се, уз одређени степен поузданости, одупру догађајима који могу да угрозе расположивост, интегритет, аутентичност, непорецивост и поверљивост података који се чувају, преносе или обрађују;

3) поверљивост је својство да податак није доступан нити откривен неовлашћеним лицима;

4) интегритет је својство очуваности изворног садржаја и комплетности податка;

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

6) аутентичност је својство које омогућава проверу да је податак створило или послало лице за које је декларисано да је ту радњу извршило;

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

8) ризик је могућност настанка штете изражена као комбинација вероватноће настанка инцидента и његових последица;

9) управљање ризиком је систематичан процес идентификовања, процене и третирања ризика како би се они одржали у прихватљивим оквирима;

10) инцидент је догађај који угрожава или нарушава информациону безбедност;

11) информациона добра су подаци, програмски код, конфигурација уређаја, техничка и корисничка документација, евиденције и други ресурси ИКТ система који подлежу заштити;

12) оператор ИКТ система је правно или физичко лице које користи ИКТ систем за обављање делатности.

## Члан 3. Циљеви акта

Циљеви доношења овог акта су:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности ИКТ система;

2. спречавање и ублажавање последица инцидената којима се угрожава или нарушава информациона безбедност;

3. подизање свести 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 праћење усклађености примењених мера заштите са овим актом.

## Члан 4. Обавеза примене

Општина, као оператор ИКТ система, одговара за безбедност ИКТ система и предузимање мера заштите прописаних овим актом.

Примена мера из овог акта обавезна је за све запослене Општина, као и за ангажоване треће стране којима је одобрен приступ ИКТ систему, у делу који се на њих односи.

[ИМЕ ОДГОВОРНОГ ЛИЦА] одговоран је за праћење примене мера из овог акта и за проверу да су информациона добра заштићена на начин утврђен овим актом и пратећим интерним документима.

## Члан 5. Одговорност запослених

Запослени су дужни да приступају информацијама и ресурсима ИКТ система искључиво ради обављања пословних активности, и да о уоченим безбедносним слабостима и инцидентима благовремено обавесте [ИМЕ ОДГОВОРНОГ ЛИЦА].

Непоштовање одредаба овог акта, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог, у складу са општим актима Општина.

## Члан 6. Организациона структура (тачка 1. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] овим актом успоставља организациону структуру информационе безбедности којом се за сваки ИКТ систем и пословни процес, укључујући вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, одређује одговорно лице задужено за његово безбедно функционисање. Надзор над информационом безбедношћу на нивоу вишег руководства врши [ИМЕ ОДГОВОРНОГ ЛИЦА], које је одговорно и за праћење усклађености са прописима о информационој безбедности. За оперативно спровођење мера информационе безбедности формира се посебна организациона јединица или се одређује лице односно тим са јасно утврђеним овлашћењима и обавезама у овој области. Додела одговорности за појединачне системе и процесе спроводи се по процедури коју утврђује [ИМЕ ОДГОВОРНОГ ЛИЦА], уз вођење евиденције о носиоцима одговорности.

Мера тренутно није испуњена, с обзиром на то да одговорност за појединачне системе и процесе није формално дефинисана и да не постоји формално задужено лице или тим за информациону безбедност, већ је одговорност на нивоу вишег руководства неформално везана за [ИМЕ ОДГОВОРНОГ ЛИЦА]. Одсуство јасно дефинисаних носилаца одговорности и формалног тела за информациону безбедност повећава ризик од неблаговременог реаговања на безбедносне инциденте и отежава координисано спровођење мера заштите, што је посебно значајно с обзиром на то да би инцидент директно угрозио могућност издавања докумената и услуга грађанима, као и поверљивост личних података из матичних књига и других евиденција. [НАЗИВ ФИРМЕ] планира успостављање формалне организационе структуре и именовање надлежног лица односно тима за информациону безбедност у наредном периоду,

[КЛИЈЕНТ ДА ДОПУНИ: рок до ког се очекује формално именовање и успостављање организационе структуре].

## Члан 7. Прикупљање података о претњама (тачка 2. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] систематски прикупља и прати податке о безбедносним претњама релевантним за своју делатност, укључујући безбедносне билтене, обавештења надлежног ЦЕРТ тима и друге релевантне изворе, ради благовременог препознавања ризика по Болнички информациони систем и друге ИКТ системе од значаја за вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За праћење претњи и размену информација са другим организацијама и индустријским групама одговоран је [ИМЕ ОДГОВОРНОГ ЛИЦА], који обезбеђује да се прикупљени подаци редовно анализирају и прослеђују надлежним лицима ради предузимања одговарајућих мера заштите. Процедура прикупљања и обраде података о претњама спроводи се континуирано, а резултати се користе као основа за ажурирање мера заштите ИКТ система.

Мера тренутно није испуњена, с обзиром на то да [НАЗИВ ФИРМЕ] не учествује у размени информација о безбедносним претњама са другим организацијама или индустријским групама нити систематски прати безбедносне билтен, ЦЕРТ обавештења и друге специјализоване изворе. Одсуство оваквог праћења повећава ризик од закаснелог препознавања нових претњи и рањивости релевантних за јавну управу, што посредно утиче на благовременост одговора на инциденте који би могли угрозити издавање докумената и услуга грађанима, као и поверљивост личних података обрађиваних у кључним пословним процесима. [КЛИЈЕНТ ДА ДОПУНИ: рок до ког се планира успостављање систематског праћења претњи и укључивање у релевантне механизме размене информација].

## Члан 8. Безбедност рада на даљину (тачка 3. члана 10. став 4. Закона)

Рад на даљину у [НАЗИВ ФИРМЕ] заснива се на употреби безбедне, енкриптоване везе (VPN или еквивалентно решење) за приступ ИКТ систему, уз примену мера заштите од неовлашћеног приступа са удаљених и мобилних уређаја. Детаљна правила уређена су посебним документом — Политика рада од куће. За примену ове мере, укључујући надзор над њеним спровођењем, одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Процедуре обухватају проверу идентитета корисника пре успостављања удаљене везе, контролу уређаја са којих се приступа систему и евидентирање удаљених приступа.

Мера тренутно није испуњена, с обзиром на то да рад на даљину не обухвата безбедну енкриптовану везу нити мере заштите од неовлашћеног приступа са удаљених и мобилних уређаја. Имајући у виду да кључни пословни процеси [НАЗИВ ФИРМЕ] — вођење матичних књига, рад писарнице и архиве, издавање уверења и

решења грађанима и наплата локалних јавних прихода — подразумевају обраду личних података грађана, одсуство безбедне везе за рад на даљину представља значајан ризик од неовлашћеног приступа и цурења података, као и од угрожавања континуитета пружања услуга грађанима у случају безбедносног инцидента.

## Члан 9. Оспособљеност лица која користе систем (тачка 4. члана 10. став 4. Закона)

Сви запослени у [НАЗИВ ФИРМЕ] који користе ИКТ системе обавезни су да прођу обуку из информационе безбедности, укључујући оспособљавање за препознавање социјалног инжењеринга, лажних позива и фишинг напада, пре стицања приступа системима и потом периодично у складу са утврђеном динамиком. Одговорност за организацију, спровођење и евидентирање обука сноси [ИМЕ ОДГОВОРНОГ ЛИЦА], као лице одговорно за праћење усклађености са прописима о информационој безбедности. Детаљна правила у погледу садржаја, учесталости и начина спровођења обука уређена су посебним документом — План обуке и подизања свести.

Обуке из информационе безбедности и оспособљавање за препознавање социјалног инжењеринга до сада нису спроведене, због чега мера тренутно није испуњена. Имајући у виду да кључни пословни процеси [НАЗИВ ФИРМЕ] — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплата локалних јавних прихода — зависе од запослених који непосредно рукују ИКТ системима и личним подацима грађана, одсуство обуке повећава вероватноћу успешних напада социјалног инжењеринга и неовлашћеног приступа подацима, што би могло директно угрозити континуитет пружања услуга грађанима и поверљивост личних података. Спровођење обука планирано је у складу са динамиком утврђеном у Плану обуке и подизања свести.

## Члан 10. Довољно ресурса (тачка 5. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] обезбеђује довољно финансијских, кадровских и техничких ресурса за спровођење мера информационе безбедности, кроз посебну буџетску линију намењену искључиво информационој безбедности, одвојену од општих трошкова информатичких послова. Планирање и предлагање обима потребних средстава спроводи се годишње, узимајући у обзир значај ИКТ система за обављање кључних пословних процеса — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За планирање, предлагање и праћење утрошка средстава намењених информационој безбедности одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које усвојени предлог буџета доставља надлежном органу управљања на одобрење.

Мера тренутно није испуњена, с обзиром на то да се трошкови информационе безбедности планирају заједно са општим ИТ трошковима, без посебне буџетске линије намењене искључиво овој области. Такво стање отежава мерљивост и

транспарентност улагања у безбедносне мере и ствара ризик да потребе информационе безбедности буду потиснуте другим информатичким приоритетима, што може утицати на правовремену набавку заштитних механизама и обуку запослених, а тиме и на континуитет кључних процеса који зависе од ИКТ система, укључујући издавање докумената грађанима и заштиту личних података.

## Члан 11. Заштита при промени послова запослених (тачка 6. члана 10. став 4. Закона)

Приступ ИКТ системима [НАЗИВ ФИРМЕ] одузима се запосленом без одлагања у случају престанка радног односа или промене радне позиције, у обиму који одговара новом статусу запосленог или његовом потпуном искључењу из система. За спровођење ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које надзире усклађеност поступања са прописима о информационој безбедности. Поступак одузимања и измене права приступа спроводи се по процедури која је ближе уређена посебним документом — Политика управљања приступом.

[КЛИЈЕНТ ДА ДОПУНИ: статус и доказ постојања процедуре за хитно одузимање приступа запосленом који напушта фирму или мења позицију, укључујући рокове поступања и носиоца оперативне одговорности]. Док ова процедура не буде јасно утврђена и документована, постоји ризик да запослени задржи неовлашћен приступ Болничком... односно ИКТ системима [НАЗИВ ФИРМЕ] након престанка радног односа или промене позиције, што би могло угрозити поверљивост личних података грађана и редовно обављање кључних процеса попут вођења матичних књига, издавања уверења и решења и наплате локалних јавних прихода.

## Члан 12. Идентификовање информационих добара (тачка 7. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] води и редовно ажурира регистар информационих добара који обухвата локације, хардвер, софтвер, запослене, информације и треће стране релевантне за рад ИКТ система. Регистар обухвата локације (зграду Општинске управе, месну канцеларију и серверску просторију), хардвер (локални сервер за писарницу и матичну књигу, радне станице, мрежну опрему и мрежне штампаче), софтвер (е-Писарницу, електронску матичну књигу, званични сајт и портал за е-услуге, софтвер за локалну пореску администрацију и буџет), запослене укључене у обраду и коришћење информационих добара, информације (личне податке грађана, кадровске податке, податке о јавним приходима и буџету, уговоре о јавним набавкама и опште акте), као и треће стране (хостинг провајдера, добављача софтвера, спољног ИТ сарадника и агенцију за обезбеђење). За вођење и ажурирање регистра информационих добара одговоран је [ИМЕ ОДГОВОРНОГ ЛИЦА], који надзире тачност и потпуност података о свим категоријама ресурса. Попис се спроводи по утврђеној процедури која обухвата идентификацију, класификацију и

периодичну ревизију информационих добара, у складу са значајем који поједина добра имају за кључне пословне процесе [НАЗИВ ФИРМЕ], пре свега вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода.

## Члан 13. Класификација података (тачка 8. члана 10. став 4. Закона)

Сви подаци које обрађује [НАЗИВ ФИРМЕ] класификују се према нивоу осетљивости, узимајући у обзир природу кључних пословних процеса — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода — као и потребу заштите поверљивости личних података грађана. Детаљна правила класификације и управљања подацима уређена су посебним документом — Политика класификације и управљања подацима, који дефинише нивое осетљивости, критеријуме разврставања и начин обележавања података. За спровођење и надзор над применом ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], у својству лица одговорног за праћење усклађености са прописима о информационој безбедности.

Политика класификације информација која дефинише различите нивое осетљивости података тренутно није донета, услед чега мера није испуњена. Непостојање формализоване класификације отежава доследно спровођење мера заштите сразмерно осетљивости података и повећава ризик од неовлашћеног приступа или неадекватног поступања са подацима који се односе на матичне књиге, издавање уверења и решења и наплату јавних прихода, чиме се посредно угрожава поверљивост личних података грађана и континуитет пружања услуга.

## Члан 14. Заштита носача података (тачка 9. члана 10. став 4. Закона)

Употреба USB портова и преносивих медијума на уређајима који чине део ИКТ система [НАЗИВ ФИРМЕ] подлеже контроли и скенирању пре сваке употребе, у циљу спречавања уноса злонамерног софтвера и неовлашћеног изношења података из система који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За примену ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које надзире усклађеност са прописима о информационој безбедности у оквиру [НАЗИВ ФИРМЕ]. Процедура подразумева обавезну проверу преносивих медијума пре прикључивања на радне станице и сервере, као и ограничавање употребе USB портова на уређајима на којима то није пословно неопходно.

Мера тренутно није примењена, с обзиром да не постоји успостављен механизам контроле или скенирања USB портова и преносивих медијума пре употребе. Одсуство ове контроле излаже ИКТ систем ризику уноса злонамерног софтвера и неовлашћеног изношења података, укључујући личне податке грађана садржане у матичним књигама и евиденцијама које [НАЗИВ ФИРМЕ] води, чиме би била

угрожена поверљивост података и континуитет пружања услуга издавања докумената грађанима.

## Члан 15. Ограничење приступа (тачка 10. члана 10. став 4. Закона)

Приступ подацима и ИКТ системима у [НАЗИВ ФИРМЕ] додељује се искључиво по принципу неопходног пословног оправдања, у обиму који је нужан за обављање конкретних радних задатака, укључујући системе који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За одобравање, периодичну проверу и одузимање права приступа одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које такође надзире примену контрола које спречавају неовлашћену измену или откривање кључних података. Детаљна правила доделе, ревизије и укидања права приступа уређена су посебним документима — Политиком управљања приступом и Политиком управљања лозинкама.

Мера тренутно није испуњена, с обзиром на то да не постоји успостављена периодична провера додељених права приступа нити механизам за уклањање непотребних овлашћења, а контроле које би спречиле неовлашћену измену или откривање кључних података такође нису успостављене. Одсуство ових контрола повећава ризик од неовлашћеног приступа личним подацима грађана и подацима из матичних књига, као и ризик од нарушавања интегритета података који су основ за издавање уверења, решења и наплату локалних јавних прихода, чиме би инцидент могао директно угрозити континуитет пружања услуга грађанима и поверљивост обрађиваних личних података. [КЛИЈЕНТ ДА ДОПУНИ: рок до ког се планира успостављање периодичне провере права приступа и контрола интегритета/поверљивости података].

## Члан 16. Одобравање овлашћеног приступа (тачка 11. члана 10. став 4. Закона)

Приступ подешавањима ИКТ система у [НАЗИВ ФИРМЕ] одобрава се искључиво овлашћеним администраторима, у складу са принципом најмање привилегије и потребом познавања. Додела, измена и укидање овлашћеног приступа спроводи се по утврђеној процедури одобравања, уз евидентирање сваког захтева и његовог одобрења. За надзор над применом ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], док су детаљна правила управљања приступом уређена посебним документом — Политика управљања приступом.

Мера тренутно није у потпуности примењена, с обзиром на то да приступ подешавањима система није ограничен искључиво на овлашћене администраторе, што представља одступање од утврђеног правила најмање привилегије. Овакво стање повећава ризик од неовлашћене измене конфигурације система који подржава вођење матичних књига, рад писарнице и архиве, издавање уверења и решења

грађанима и наплату локалних јавних прихода, чиме се угрожава расположивост и интегритет ових услуга, као и поверљивост личних података грађана. [КЛИЈЕНТ ДА ДОПУНИ: рок и конкретне активности за успостављање ограничења приступа подешавањима система искључиво на овлашћене администраторе].

## Члан 17. Одговорност корисника (тачка 12. члана 10. став 4. Закона)

Сваки корисник ИКТ система у [НАЗИВ ФИРМЕ] лично одговара за начин коришћења додељене ИТ опреме, налога и приступа интернету, као и за поступање у складу са правилима о коришћењу лозинки. Лозинке су строго личне, њихово дељење је забрањено, а детаљна правила управљања лозинкама уређена су посебним документом — Политика управљања лозинкама. Дозвољено коришћење ИТ опреме и интернета уређује се посебним документом — Политика прихватљиве употребе ИТ опреме, који је саставни основ за утврђивање одговорности корисника у овој области. За надзор над применом ове мере и праћење усклађености са прописима о информационој безбедности одговоран је [ИМЕ ОДГОВОРНОГ ЛИЦА].

Политика о дозвољеном коришћењу ИТ опреме и интернета у овом тренутку није усвојена, због чега мера одговорности корисника није у потпуности примењена, иако је обавеза личне употребе лозинки без дељења налога успостављена и примењује се. Одсуство формализоване политике прихватљиве употребе повећава ризик од неовлашћеног или ненаменског коришћења ИКТ ресурса, што је, с обзиром на то да системи [НАЗИВ ФИРМЕ] подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, од значаја за поверљивост личних података грађана и континуитет пружања јавних услуга. Усвајање Политике прихватљиве употребе ИТ опреме очекује се у наредном периоду, након чега ће ова мера бити у потпуности примењена.

## Члан 18. Криптографске контроле (тачка 13. члана 10. став 4. Закона)

Осетљиви подаци у ИКТ систему [НАЗИВ ФИРМЕ], укључујући податке из матичних књига, евиденција писарнице и архиве, као и податке везане за наплату локалних јавних прихода, штите се применом криптографских контрола како у стању мировања тако и приликом преноса, а резервне копије података енкриптују се и периодично се проверава успешност њиховог обнављања. За примену и надзор над криптографским контролама, укључујући одлучивање о избору криптографских алгоритама и управљање криптографским кључевима, одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Процедуре обухватају одређивање категорија података који подлежу обавезној енкрипцији, начин чувања и обнове кључева, као и редовно тестирање поступка обнављања резервних копија, уз периодично преиспитивање отпорности примењених криптографских решења на будуће претње, укључујући развој квантног рачунарства.

[КЛИЈЕНТ ДА ДОПУНИ: одговори на питања 2.8 и 3.20/3.21 из процене ризика евидентирани су као „недефинисано“, због чега није могуће утврдити да ли су осетљиви подаци у потпуности енкриптовани, да ли се тестирање обнављања резервних копија заиста спроводи, нити да ли је размотрен ризик од будућег пробијања енкрипције квантним рачунарством — потребно је допунити конкретне податке о примењеним криптографским мерама и резултатима тестирања]. Процена утицаја: с обзиром на то да систем обрађује личне податке грађана и податке релевантне за наплату јавних прихода, недостатак поузданих информација о примени криптографских контрола и тестирању обнављања резервних копија представља повећан ризик по поверљивост и расположивост података, као и по континуитет пружања услуга грађанима у случају безбедносног инцидента.

## Члан 19. Заштита од отицања података (тачка 14. члана 10. став 4. Закона)

Заштита од отицања података у [НАЗИВ ФИРМЕ] обухвата скуп техничких и организационих контрола којима се спречава неовлашћено откривање, дељење или измена осетљивих и кључних података, укључујући податке из матичних књига, предмета писарнице и архиве, као и податке неопходне за издавање уверења и решења грађанима. Правила о дозвољеним начинима дељења осетљивих података путем електронске поште, штампе и других канала, као и класификација података према нивоу осетљивости, уређена су посебним документима — Политиком класификације и управљања подацима и Политиком прихватљиве употребе ИТ опреме. За примену мере заштите од отицања података, укључујући успостављање техничких контрола које спречавају неовлашћену измену или откривање кључних података, одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Примена ових правила надзире се кроз редовно праћење усклађености са прописима о информационој безбедности, за шта је такође задужено [ИМЕ ОДГОВОРНОГ ЛИЦА].

Мера тренутно није испуњена, с обзиром на то да правила о дељењу осетљивих података путем електронске поште и штампе нису дефинисана, нити постоји техничка контрола која спречава неовлашћену измену или откривање кључних података. Одсуство ових контрола повећава ризик од неовлашћеног откривања личних података грађана и података из матичних књига, као и ризик од нарушавања интегритета података који се користе у поступцима издавања уверења и решења, што може директно угрозити континуитет пружања услуга грађанима и поверљивост обрађених личних података. [КЛИЈЕНТ ДА ДОПУНИ: рок и план увођења правила о дељењу осетљивих података и техничких контрола за спречавање неовлашћене измене или откривања кључних података].

## Члан 20. Физичка заштита објеката (тачка 15. члана 10. став 4. Закона)

Просторије са ИКТ опремом у [НАЗИВ ФИРМЕ] штите се од пожара, продора воде и прекомерне влажности и прашине путем одговарајућих система детекције и гашења пожара, заштите од поплава и цурења и климатизације, док се физичко обезбеђење остварује бравама, алармним системом и видео надзором. Опрема се додатно штити мерама уземљења и адекватног размештаја у односу на изворе електромагнетних сметњи, а температура и влажност у серверској просторији подлежу редовном надзору ради благовременог откривања одступања од прописаних услова. За примену ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које обезбеђује спровођење процедура физичке заштите и надзора услова у просторијама са опремом. Процедуре обухватају редовну проверу исправности система заштите, контролу приступа просторијама и периодичну проверу стања заштите опреме од електромагнетних сметњи.

Мера тренутно није у потпуности примењена јер не постоји успостављен систем редовног надгледања температуре и влажности у серверској просторији, нити је потврђена заштита опреме од електромагнетних сметњи путем уземљења и одговарајућег размештаја. Одсуство континуираног надзора микроклиматских услова повећава ризик од неопаженог прегревања или прекомерне влажности који могу довести до отказа опреме, док неадекватна заштита од електромагнетних сметњи може утицати на стабилност и поузданост рада система. Имајући у виду да о раду ИКТ система зависе кључни процеси [НАЗИВ ФИРМЕ] — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплата локалних јавних прихода — ово одступање представља ризик од прекида пружања услуга грађанима и потенцијалног угрожавања поверљивости и доступности личних података.

## Члан 21. Заштита од губитка (тачка 16. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] примењује заштиту од губитка података кроз комбинацију техничких и организационих мера које обухватају резервно напајање кључне опреме, процедуру за пријаву губитка или крађе опреме, као и израду резервних копија података значајних за вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. Резервне копије се израђују редовно, а њихова израда и чување организују се тако да се обезбеди могућност обнављања кључних пословних процеса у случају инцидента. За примену ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које прати и усклађеност примене мере са прописима о информационој безбедности. Процедура за пријаву губитка или крађе опреме примењује се на сву опрему која учествује у обради података од значаја за рад [НАЗИВ ФИРМЕ].

Мера није у потпуности примењена јер резервне копије нису заштићене од брисања са компромитованог налога, односно нису организоване као оффлине или на други начин одвојене копије, нити постоје мере специфично усмерене против рансомвер

напада попут непроменљивих копија или сегментације мреже, док енкрипција осетљивих података и тестирање успешности обнављања резервних копија нису дефинисани. Овакво стање излаже [НАЗИВ ФИРМЕ] ризику да у случају компромитације налога или рансомвер напада резервне копије буду избрисане или онемогућене за обнављање, што би директно угрозило могућност издавања докумената и пружања услуга грађанима, као и поверљивост и доступност личних података грађана. Отклањање овог одступања планира се кроз увођење одвојених, оффлине резервних копија и мера заштите од рансомвер напада, уз накнадно утврђивање конкретног рока од стране [ИМЕ ОДГОВОРНОГ ЛИЦА].

## Члан 22. Исправност средстава (тачка 17. члана 10. став 4. Закона)

Исправност медијума за складиштење података у [НАЗИВ ФИРМЕ] проверава се редовним поступком контроле функционалног стања уређаја и носача података на којима се чувају подаци из кључних пословних процеса, укључујући вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За спровођење ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које прати усклађеност са прописима о информационој безбедности и стара се о доследној примени утврђених процедура. Провера обухвата периодичну дијагностику стања медијума, евидентирање уочених неправилности и предузимање мера за благовремену замену или поправку неисправних средстава, у складу са интерним процедурама које се овим актом успостављају.

На основу достављених података није могуће утврдити да ли се поступак редовне провере исправности медијума за складиштење података тренутно спроводи, нити у ком обиму, будући да је одговор на релевантно питање из процене ризика означен као непознат. Овакво одсуство поуздане информације о стању примене мере представља ризик по расположивост и интегритет података од значаја за обављање послова из надлежности [НАЗИВ ФИРМЕ], укључујући податке неопходне за издавање докумената и услуга грађанима, те по поверљивост личних података садржаних у тим системима. [КЛИЈЕНТ ДА ДОПУНИ: тачан статус спровођења провере исправности медијума за складиштење података, учесталост провере и доказ о њеном спровођењу].

## Члан 23. Процедуре за рачунарство у клауду (тачка 18. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] применом ове мере успоставља обавезу да се коришћење услуга рачунарства у облаку заснива на јасно утврђеној подели безбедносних обавеза између [НАЗИВ ФИРМЕ] и „cloud“ провајдера, укључујући проверу независних безбедносних сертификата провајдера, познавање локације физичког смештаја података и могућност промене провајдера без угрожавања континуитета пословних процеса. За примену ове мере одговоран је [ИМЕ ОДГОВОРНОГ ЛИЦА], који је задужен

и за праћење усклађености са прописима о информационој безбедности у овом домену. Процедуре обухватају анализу уговора и услова коришћења услуга „cloud“ провајдера, проверу постојања релевантних сертификата (нпр. ISO 27001), утврђивање јурисдикције у којој се подаци обрађују и чувају, као и процену могућности и трошкова евентуалне миграције ка другом провајдеру.

На основу достављених доказа није могуће утврдити да ли је ова мера примењена, с обзиром на то да су сви релевантни одговори у процени ризика евидентирани као „не знам", те је статус мере оцењен као нејасан. [КЛИЈЕНТ ДА ДОПУНИ: подаци о конкретном „cloud“ провајдеру, постојећим уговорним одредбама о подели одговорности, сертификатима провајдера и локацији складиштења података]. Имајући у виду да кључни пословни процеси [НАЗИВ ФИРМЕ] — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплата локалних јавних прихода — зависе од ИКТ система, недостатак јасних сазнања о безбедносним обавезама провајдера, сертификацији и локацији података представља значајан ризик по поверљивост, интегритет и доступност података, као и по континуитет пружања услуга грађанима, до тренутка допуне и верификације наведених података.

## Члан 24. Праћење система (тачка 19. члана 10. став 4. Закона)

Праћење ИКТ система у [НАЗИВ ФИРМЕ] обухвата континуирани надзор искоришћености капацитета система, укључујући простор за складиштење података и меморијске ресурсе, као и благовремено уочавање неуобичајених активности које могу указивати на безбедносни инцидент. Овим актом успоставља се обавеза праћења рада система који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, с обзиром на то да престанак рада тих система директно угрожава пружање услуга грађанима и поверљивост личних података. За примену ове мере, укључујући дефинисање процедура праћења и плана поступања у случају престанка рада кључног система, одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Процедуре праћења и поступања у случају неуобичајене активности или престанка рада система ближе се уређују интерним упутствима која доноси одговорно лице.

[КЛИЈЕНТ ДА ДОПУНИ: конкретан опис да ли и на који начин се тренутно прати искоришћеност капацитета система, да ли постоји механизам за уочавање неуобичајене активности и да ли постоји усвојен план за случај престанка рада кључног система]. На основу достављених података није могуће утврдити обим примене мере, због чега се не може извршити ни потпуна процена утицаја евентуалног одступања на безбедност ИКТ система; с обзиром на то да кључни пословни процеси — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплата локалних јавних прихода — зависе од непрекидног рада ИКТ система, непостојање јасно дефинисаног праћења капацитета

и неуобичајених активности представља потенцијални ризик од неблаговременог откривања инцидента и продуженог прекида пружања услуга грађанима.

## Члан 25. Ограничење приступа веб презентацијама (тачка 20. члана 10. став 4. Закона)

Приступ запослених [НАЗИВ ФИРМЕ] интернет садржајима са радних станица и из ИКТ система ограничава се и филтрира на начин којим се спречава приступ потенцијално малициозним и непримереним веб презентацијама. Примена ове мере обухвата све запослене који користе ИТ опрему и приступ интернету у оквиру обављања пословних процеса, укључујући вођење матичних књига, рад писарнице и архиве и издавање уверења и решења грађанима. За спровођење и надзор над применом ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Детаљна правила уређена су посебним документом — Политика прихватљиве употребе ИТ опреме.

На основу расположивих података није могуће утврдити да ли је и у ком обиму успостављено техничко филтрирање или контрола приступа потенцијално малициозним веб сајтовима, с обзиром да је у процени ризика одговор клијента на ово питање био „не знам". [КЛИЈЕНТ ДА ДОПУНИ: да ли постоји техничко решење (нпр. web филтер, proxy, ДНС филтрирање) за ограничавање приступа малициозним сајтовима, и ко је надлежан за његову конфигурацију и ажурирање]. До разјашњења овог стања, постоји ризик да запослени могу неометано приступати веб локацијама које представљају вектор за уношење малвера или „phishing“ напада, што би, с обзиром на то да ИКТ систем [НАЗИВ ФИРМЕ] подржава издавање докумената грађанима и обраду личних података, могло угрозити доступност услуга и поверљивост података у информационом систему.

## Члан 26. Заштита од злонамерног софтвера (тачка 21. члана 10. став 4. Закона)

Заштита од злонамерног софтвера спроводи се на свим уређајима у оквиру ИКТ система [НАЗИВ ФИРМЕ], укључујући радне станице и сервере који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. Решење за заштиту од злонамерног софтвера инсталира се, ажурира и надзире као обавезан елемент безбедносне конфигурације сваког уређаја пре његовог стављања у продукциону употребу. За примену и надзор над овом мером одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које прати стање заштите на свим уређајима и предузима мере у случају детекције злонамерне активности. Процедуре обухватају редовно ажурирање дефиниција претњи, периодичну проверу статуса заштите на уређајима и поступање у случају откривања инфекције, укључујући изолацију угроженог уређаја ради спречавања ширења на остале делове ИКТ система.

## Члан 27. Резервне копије података (тачка 22. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] овим актом успоставља обавезу редовног креирања резервних копија података из свих ИКТ система који подржавају кључне пословне процесе, укључујући вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, како би се обезбедила могућност опоравка података у случају безбедносног инцидента, губитка или оштећења података. За организовање, спровођење и редовну проверу поступка израде резервних копија одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Резервне копије се креирају према утврђеној динамици, чувају се на начин који обезбеђује њихову доступност и заштиту од неовлашћеног приступа, а њихова исправност и могућност враћања података проверавају се периодично ради потврде поузданости поступка опоравка.

## Члан 28. Чување података о догађајима (тачка 23. члана 10. став 4. Закона)

Евиденције (логови) о активностима у ИКТ системима [НАЗИВ ФИРМЕ] чувају се у роковима и на начин који омогућава накнадну проверу активности корисника и системских процеса, а приступ тим евиденцијама и њихова заштита од неовлашћене измене или брисања уређују се као обавезан део рада са ИКТ системом. За примену ове мере, укључујући одређивање рокова чувања евиденција и контролу приступа евиденцијама, одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Провера евиденција врши се периодично, а сваки приступ евиденцијама од стране лица која нису овлашћена за њихову измену или брисање сматра се безбедносним инцидентом који се пријављује и обрађује у складу са интерним процедурама.

Мера тренутно није испуњена јер евиденције активности нису заштићене од измене или брисања од стране неовлашћених лица, а поступак редовног чувања и провере евиденција није дефинисан. Овакво стање носи повећан ризик од неовлашћеног прикривања трагова злоупотребе или безбедносног инцидента, што је нарочито значајно с обзиром на то да се у систему обрађују лични подаци грађана у поступцима вођења матичних књига, издавања уверења и решења, као и наплате локалних јавних прихода — немогућност поуздане реконструкције догађаја директно угрожава способност [НАЗИВ ФИРМЕ] да утврди узрок и обим евентуалног инцидента и да благовремено заштити поверљивост и интегритет тих података.

## Члан 29. Интегритет софтвера (тачка 24. члана 10. став 4. Закона)

Интегритет софтвера у [НАЗИВ ФИРМЕ] обезбеђује се преузимањем софтвера искључиво из поузданих, званичних извора, чиме се спречава уношење неовлашћених или злонамерних измена у ИКТ системе који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За трајне измене важних података у овим

системима примењује се контрола верзија, односно поступак потврде пре њиховог коначног уношења, како би се очувала тачност и поузданост података од значаја за остваривање права грађана. За примену ове мере, укључујући надзор над изворима софтвера и поступцима контроле измена података, одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Процедуре примене ове мере спроводе се у оквиру редовних активности одржавања и администрације ИКТ система.

[КЛИЈЕНТ ДА ДОПУНИ: статус и доказ примене контроле верзија односно поступка потврде пре трајних измена важних података, с обзиром на то да је одговор на питање 3.7 означен као недефинисано]. Док се овај податак не прецизира, не може се са сигурношћу утврдити да ли је мера у погледу контроле измена података примењена у пуном обиму, што представља ризик по интегритет података у кључним пословним процесима [НАЗИВ ФИРМЕ], укључујући могућност неовлашћене или непримећене измене података релевантних за издавање докумената грађанима и наплату јавних прихода.

## Члан 30. Заштита од злоупотребе слабости (тачка 25. члана 10. став 4. Закона)

Заштита ИКТ система од злоупотребе слабости спроводи се редовним ажурирањем софтвера, оперативних система и свих мрежних уређаја, укључујући мрежне штампаче и скенере, ради отклањања безбедносних пропуста који могу бити искоришћени за неовлашћени приступ или нарушавање рада система. Мрежни уређаји обавезно се штите одговарајућом лозинком, а приступ њиховим административним функцијама ограничава се на овлашћена лица. За примену ове мере, укључујући планирање и спровођење ажурирања и контролу заштите мрежних уређаја, одговоран је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Процедуре ажурирања спроводе се по утврђеном распореду, уз приоритетно поступање по критичним безбедносним исправкама.

Мера тренутно није испуњена, с обзиром на то да поступак редовног ажурирања софтвера и оперативних система није дефинисан, а мрежни штампачи и скенери нису ажурирани нити заштићени лозинком. Овакво стање излаже [НАЗИВ ФИРМЕ] повећаном ризику од злоупотребе познатих безбедносних слабости, што с обзиром на то да кључни пословни процеси — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплата локалних јавних прихода — зависе од ИКТ система, може довести до прекида пружања услуга грађанима и угрожавања поверљивости личних података који се обрађују у тим процесима. [КЛИЈЕНТ ДА ДОПУНИ: рок до када се планира успостављање процедуре редовног ажурирања и заштите мрежних уређаја].

## Члан 31. Заштита при ревизорском тестирању (тачка 26. члана 10. став 4. Закона)

Тестирање ИКТ система путем ревизорских провера и пенетрационог тестирања спроводи се плански, у обиму који обухвата системе од значаја за вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, ради провере отпорности ових система на безбедносне претње. За успостављање и спровођење политике редовног тестирања пенетрације, као и за надзор над њеном применом, одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Налази добијени тестирањем евидентирају се и користе као основ за предузимање корективних мера у циљу отклањања утврђених рањивости.

Политика редовног тестирања пенетрације тренутно није успостављена, услед чега мера није испуњена. Одсуство овакве политике онемогућава благовремено откривање рањивости у системима који подржавају издавање докумената и услуга грађанима, чиме се повећава ризик од неовлашћеног приступа и угрожавања поверљивости личних података грађана, а самим тим и ризик по континуитет кључних пословних процеса [НАЗИВ ФИРМЕ].

## Члан 32. Заштита података у мрежама (тачка 27. члана 10. став 4. Закона)

Мрежни саобраћај и комуникација у оквиру ИКТ система [НАЗИВ ФИРМЕ], укључујући VPN конекције и пренос фајлова, штите се применом одговарајућих криптографских механизама којима се обезбеђује поверљивост и интегритет података у преносу, а мера се примењује на све канале комуникације којима се размењују подаци везани за вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За примену ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које надзире спровођење техничких контрола енкрипције мрежног саобраћаја и усклађеност са овим актом. Процедуре обухватају идентификацију свих канала преноса података, успостављање енкрипције VPN конекција и преноса фајлова, као и редовну проверу исправности примењених криптографских решења.

Енкрипција мрежног саобраћаја и комуникације, укључујући VPN конекције и пренос фајлова, тренутно није успостављена, што је утврђено у поступку процене ризика. Одсуство ове заштите излаже ризику поверљивост и интегритет личних података грађана који се обрађују у оквиру кључних пословних процеса [НАЗИВ ФИРМЕ], као и података који се преносе мрежом у вези са издавањем уверења и решења, вођењем матичних књига и наплатом локалних јавних прихода, чиме се повећава ризик од неовлашћеног приступа и компромитовања података у преносу. [КЛИЈЕНТ ДА ДОПУНИ: рок и план увођења енкрипције мрежног саобраћаја и VPN комуникације].

## Члан 33. Безбедност података у комуникацији (тачка 28. члана 10. став 4. Закона)

Мрежни саобраћај и комуникација који обухватају пренос података у оквиру ИКТ система [НАЗИВ ФИРМЕ], укључујући VPN конекције и пренос фајлова, штите се применом одговарајућих криптографских механизама којима се обезбеђује поверљивост и интегритет података у преносу, а ова заштита примењује се на све канале комуникације којима се размењују подаци везани за вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За примену ове мере, укључујући одређивање техничких решења за енкрипцију и надзор над њиховим функционисањем, одговоран је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Процедуре примене обухватају идентификацију свих канала преноса података који захтевају криптографску заштиту, имплементацију енкрипције мрежног саобраћаја и редовну проверу исправности примењених криптографских механизама.

Мера тренутно није испуњена, с обзиром на то да мрежни саобраћај и комуникација, укључујући VPN и пренос фајлова, нису заштићени енкрипцијом. Имајући у виду да се путем ИКТ система обрађују лични подаци грађана у поступцима вођења матичних књига, издавања уверења и решења и наплате локалних јавних прихода, одсуство енкрипције у комуникацији представља значајан ризик од неовлашћеног увида, пресретања или измене података у преносу, чиме се угрожава поверљивост и интегритет података грађана и поузданост пружања јавних услуга. [КЛИЈЕНТ ДА ДОПУНИ: рок до ког се планира имплементација енкрипције мрежног саобраћаја и VPN/преноса фајлова].

## Члан 34. Захтеви током животног циклуса (тачка 29. члана 10. став 4. Закона)

Измене на ИКТ системима у [НАЗИВ ФИРМЕ] спроводе се искључиво кроз дефинисан процес управљања променама, који обухвата проверу од стране другог лица независног од извршиоца измене, претходно тестирање измена ван продукционог окружења и верификацију подешавања система пре пуштања у рад. За спровођење и надзор над овим процесом одговоран је [ИМЕ ОДГОВОРНОГ ЛИЦА], у својству лица одговорног за праћење усклађености са прописима о информационој безбедности. Процедуре обухватају обавезно документовање захтева за измену, одобрење од стране овлашћеног лица, независну проверу измене пре имплементације и тестирање у контролисаном окружењу пре преласка у продукцију.

[КЛИЈЕНТ ДА ДОПУНИ: конкретан опис да ли и у којој мери постоји формализована процедура провере „другог пара очију“, тестирања измена и верификације подешавања пре пуштања у продукцију, уз доказе о примени, с обзиром да су одговори из процене ризика на питања 3.2, 3.4 и 3.11 евидентирани као „недефинисано“]. До коначног утврђивања и документовања ових процедура, постоји

ризик да измене на ИКТ системима, укључујући системе који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, буду уведене без адекватне независне контроле и тестирања, што може довести до грешака у раду система, прекида пружања услуга грађанима или угрожавања поверљивости и интегритета личних података.

## Члан 35. Заштита тест података (тачка 30. члана 10. став 4. Закона)

Приликом тестирања ИКТ система у [НАЗИВ ФИРМЕ] користе се искључиво подаци који не садрже стварне личне или осетљиве податке грађана, односно тест подаци који садрже такве категорије података подлежу посебним мерама заштите једнаким онима које се примењују на продукционе податке. Одговорност за примену ове мере сноси [ИМЕ ОДГОВОРНОГ ЛИЦА], које надзире усклађеност поступања са тест подацима са прописима о заштити података о личности и информационој безбедности. Процедура обухвата претходну анонимизацију или псеудонимизацију података из продукционих система пре њиховог коришћења у тест окружењима, као и контролу приступа тест окружењима која одговара осетљивости података који се у њима обрађују, узимајући у обзир да кључни процеси попут вођења матичних књига и издавања уверења и решења грађанима подразумевају обраду личних података високе осетљивости.

[КЛИЈЕНТ ДА ДОПУНИ: статус и доказ примене ове мере — потребно је утврдити да ли се у тест окружењима тренутно користе стварни лични/осетљиви подаци из продукционих система, којим поступком се врши анонимизација или псеудонимизација уколико постоји, и до ког рока ће поступак заштите тест података бити формално успостављен и документован]. Док се ова околност не разјасни и процедура не потврди доказима, постоји ризик неовлашћеног откривања личних података грађана у тест окружењима која по правилу имају слабији ниво контроле приступа од продукционих система, што би, с обзиром на природу података које [НАЗИВ ФИРМЕ] обрађује у оквиру вођења матичних књига и издавања докумената грађанима, представљало значајан утицај на поверљивост података о личности.

## Члан 36. Процедуре чувања и брисања (тачка 31. члана 10. став 4. Закона)

Подаци у ИКТ системима [НАЗИВ ФИРМЕ], укључујући податке из вођења матичних књига, рада писарнице и архиве, као и податке везане за издавање уверења, решења и наплату локалних јавних прихода, чувају се и бришу у складу са прописаним и уговореним роковима чувања, а по истеку тих рокова подаци се неповратно уништавају, укључујући и податке код спољних провајдера услуга по раскиду уговора. За примену ове мере, успостављање рокова чувања по врстама података и контролу неповратног брисања одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Процедуре обухватају евидентирање рокова чувања за поједине категорије података, поступак

неповратног брисања по истеку рока, као и проверу да ли уговори са провајдерима садрже одредбе о начину и доказивању трајног брисања података по престанку уговорног односа.

Статус примене ове мере оцењен је као нејасан, с обзиром на то да одговори прикупљени у поступку процене ризика указују да начин неповратног брисања података по истеку рока чувања није дефинисан, као ни да ли и на који начин провајдер трајно брише податке по раскиду уговора. Недостатак јасно утврђеног и документованог поступка брисања података, као и одсуство информација о поступању ангажованог провајдера, представља ризик од неовлашћеног задржавања или цурења личних података грађана након истека сврхе обраде, што може угрозити поверљивост података и усклађеност са прописима о заштити података о личности. [КЛИЈЕНТ ДА ДОПУНИ: тачан статус дефинисаности интерног поступка брисања података, назив и одредбе уговора са провајдером у погледу брисања података, и рок до ког ће ова питања бити разјашњена и документована].

## Члан 37. Заштита средстава доступних пружаоцима (тачка 32. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] овим актом прописује да се средства и ресурси доступни пружаоцима услуга (добављачима хардвера, софтвера и других ИКТ компоненти) штите кроз уговорно дефинисање обавеза у погледу безбедности, заштите података и поступања у случају безбедносног инцидента, као и кроз претходну проверу безбедносне поузданости добављача пре њиховог увођења у ИКТ систем. За примену ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које прати усклађеност уговорних односа са трећим странама са захтевима информационе безбедности. Детаљна правила уређена су посебним документом — Политика управљања трећим странама.

[КЛИЈЕНТ ДА ДОПУНИ: статус и доказ примене ове мере — конкретно, да ли је уговорима са провајдерима регулисано поступање по захтеву државних органа и пружање подршке у случају инцидента, да ли су потписани уговори о обради личних података са добављачима и да ли се спроводи провера безбедносне поузданости добављача хардвера/софтвера пре увођења]. На основу доступних података из процене ризика није могуће утврдити степен примене ове мере, с обзиром на то да су одговори клијента на релевантна питања означени као „не знам" односно „недефинисано". Имајући у виду да кључни процеси [НАЗИВ ФИРМЕ] (вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима, наплата локалних јавних прихода) зависе од ИКТ система и укључују обраду личних података грађана, недостатак јасно дефинисаних уговорних обавеза према пружаоцима и непровера поузданости добављача представља потенцијални ризик по поверљивост података и континуитет пружања услуга грађанима.

## Члан 38. Одржавање уговореног нивоа услуге (тачка 33. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] овим актом прописује да се ниво услуге уговорен са добављачима ИКТ услуга, укључујући услове под којима је могућа замена провајдера без неприхватљивог поремећаја пословних процеса, редовно проверава и документује, како би се обезбедио континуитет кључних процеса који зависе од ИКТ система. За примену ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које прати усаглашеност уговорених нивоа услуге са пословним потребама [НАЗИВ ФИРМЕ]. Процедуре провере услова раскида и замене добављача, као и друга питања односа са трећим странама, уређене су посебним документом — Политика управљања трећим странама.

На основу доступних доказа није могуће са сигурношћу утврдити да ли би [НАЗИВ ФИРМЕ] могла да промени „cloud“ провајдера без значајног поремећаја пословања, с обзиром на то да одговор на ово питање у процени ризика гласи „не знам“. Оваква неизвесност представља ризик за континуитет кључних пословних процеса — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода — јер у случају потребе за хитном заменом провајдера не постоји потврђена спремност да се то спроведе без прекида услуга према грађанима. [КЛИЈЕНТ ДА ДОПУНИ: конкретан статус уговора о нивоу услуге са „cloud“ провајдером, постојање излазне стратегије (exit план) и процена могућности и времена потребног за замену провајдера].

## Члан 39. Превенција инцидената (тачка 34. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] примењује мере превенције безбедносних инцидената у обиму који обухвата заштиту ИКТ система од преоптерећења великим бројем захтева (DoS напади), мере специфично усмерене против рансомвер напада, укључујући непроменљиве резервне копије и сегментацију мреже, као и уговорно дефинисање поступања по захтеву државних органа и пружања подршке у случају инцидента од стране трећих страна са којима [НАЗИВ ФИРМЕ] сарађује. За примену ове мере одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА], које прати усклађеност са прописима о информационој безбедности и стара се о успостављању техничких и организационих мера превенције инцидената. Процедуре поступања у случају безбедносног инцидента, укључујући улоге и кораке реаговања, детаљно су уређене посебним документом — План реаговања на инциденте.

Мера тренутно није испуњена, с обзиром на то да не постоји заштита од DoS напада нити специфичне мере против рансомвер напада попут непроменљивих копија података и сегментације мреже, док статус уговорне дефинисаности поступања по захтеву државних органа и подршке у случају инцидента није утврђен. Имајући у виду да кључни пословни процеси [НАЗИВ ФИРМЕ] — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплата локалних

јавних прихода — у потпуности зависе од расположивости ИКТ система, одсуство ових превентивних мера представља значајан ризик по континуитет пружања услуга грађанима и по поверљивост личних података који се обрађују, посебно у случају рансомвер напада или намерног онемогућавања доступности сервиса. Процењени утицај овог одступања на безбедност ИКТ система оцењује се као висок, те је успостављање недостајућих мера приоритет у наредном периоду.

## Члан 40. Континуитет послова (тачка 35. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] овим актом успоставља континуитет рада кључних ИКТ система који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, кроз планирање опоравка од катастрофе и обезбеђење редундансе критичне инфраструктуре, опреме и комуникационих веза. Детаљна правила уређена су посебним документима — План континуитета пословања (BCP) и План опоравка од катастрофе (DRP). За примену ове мере, укључујући активирање планова опоравка, одређивање замена за кључне ИТ улоге и надзор над неуобичајеном активношћу која може угрозити рад кључних система, одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Поступање у случају престанка рада кључног система, отказа хардвера/софтвера или губитка примарне интернет/телеком везе спроводи се у складу са процедурама дефинисаним у наведеним плановима.

Мера тренутно није испуњена, с обзиром на то да не постоји усвојен план опоравка за случај велике природне непогоде, није обезбеђена резервна опрема нити резервна интернет/телеком веза, а улоге замене за кључне ИТ функције и поступци за уочавање неуобичајене активности и престанка рада кључног система нису дефинисани. Овакво одступање носи висок утицај на безбедност ИКТ система [НАЗИВ ФИРМЕ], јер би наступање природне непогоде, квара хардвера/софтвера или прекида телекомуникационе везе довело до обуставе издавања докумената и услуга грађанима, као и до ризика по поверљивост и доступност личних података грађана садржаних у матичним књигама и другим евиденцијама. [КЛИЈЕНТ ДА ДОПУНИ: рок до ког се планира усвајање и имплементација BCP и DRP докумената, носилац активности и статус набавке резервне опреме и везе].

## Члан 41. Усвајање докумената (тачка 36. члана 10. став 4. Закона)

[НАЗИВ ФИРМЕ] овим актом усваја релевантна интерна документа којима се уређује безбедност ИКТ система од посебног значаја, укључујући писана упутства за рад запослених са кључним системима, у обиму који обухвата све пословне процесе који зависе од ИКТ система, а нарочито вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. За усвајање, ажурирање и доступност ових докумената запосленима одговорно је [ИМЕ ОДГОВОРНОГ ЛИЦА]. Усвојена документа примењују се кроз процедуру упознавања

запослених са њиховом садржином приликом почетка рада на кључним системима, као и приликом сваке накнадне измене докумената.

Статус усклађености са овом мером је нејасан, будући да је на питање о постојању писаних упутстава за рад са кључним системима дат одговор „недефинисано", чиме није утврђено да ли су таква документа заиста усвојена и у ком обиму су доступна запосленима. Оваква неизвесност у погледу постојања и примене писаних упутстава носи ризик по безбедност ИКТ система, јер запослени могу поступати недоследно или супротно утврђеним безбедносним правилима приликом рада са системима који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, што може угрозити како континуитет пружања услуга грађанима тако и поверљивост личних података. [КЛИЈЕНТ ДА ДОПУНИ: тачан статус постојања писаних упутстава за рад са кључним системима, назив и обухват тих докумената, као и доказ о њиховом усвајању и достављању запосленима].

## Члан 42. Мултифакторска аутентификација (тачка 37. члана 10. став 4. Закона)

Мултифакторска аутентификација примењује се као обавезан метод верификације идентитета корисника приликом приступа кључним системима [НАЗИВ ФИРМЕ], укључујући системе који подржавају вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. Одговорност за увођење и надзор над применом мултифакторске аутентификације сноси [ИМЕ ОДГОВОРНОГ ЛИЦА], у оквиру опште одговорности за надзор над информационом безбедношћу. Процедуре за управљање креденцијалима и аутентификационим факторима спроводе се у складу са интерним документом Политика управљања лозинкама, који се у делу који се односи на додатне факторе аутентификације допуњује овим актом.

Мера тренутно није примењена, с обзиром на то да приступ кључним системима не захтева вишефакторску аутентикацију, што представља одступање од прописаног правила из претходног пасуса. Ово одступање излаже системе који подржавају издавање докумената и услуга грађанима повећаном ризику од неовлашћеног приступа заснованог искључиво на компромитацији лозинке, чиме се угрожава поверљивост личних података грађана и континуитет вршења јавних овлашћења [НАЗИВ ФИРМЕ]. [КЛИЈЕНТ ДА ДОПУНИ: рок и план увођења мултифакторске аутентификације за кључне системе].

## Ступање на снагу

Овај акт ступа на снагу даном усвајања од стране надлежног органа управљања Општина, а примењује се од наредног дана.

У _____, ___.___._____. године

Број: _____

М.П.

Овлашћено лице:

_____