Анализа ризика информационе безбедности — Општина

Корисник: Општина

Анализу припремио: Биро за дигиталну безбедност д.о.о.

ПОВЕРЉИВО И ИНТЕЛЕКТУАЛНА СВОЈИНА БДБ — документ фирме „Општина“ садржи анализу безбедносних ризика ИКТ система. Документ се користи искључиво за интерне потребе крајњег корисника; неовлашћено умножавање или дистрибуција трећим лицима није дозвољено.

Датум израде: 08.11.2026.

Садржај

- Увод
- Методологија процене ризика
- Нивои ризика
- Налази по тематским областима
- Управљање и организациона структура
- Политике безбедности и класификација
- Управљање приступом и идентитетима
- Прихватљиво коришћење и свест запослених
- Техничка заштита мреже и система
- Управљање подацима и складиштењем
- Мониторинг и евиденције
- „Cloud“ сервиси и спољни ИТ провајдери
- Реаговање на инциденте и опоравак
- Физичка безбедност
- Однос са трећим странама
- Лиценцирање софтвера и легалност система
- Преглед нивоа ризика по областима
- Закључак
- Прилози

Увод

На основу Закона о информационој безбедности („Сл. гласник РС“, бр. 91/2025), оператор ИКТ система од посебног значаја дужан је да изврши процену ризика и на

основу ње изради Акт о безбедности ИКТ система. Ова анализа представља ту процену ризика за „Општина“.

Документ је израђен применом методологије из Правилника о општој методологији за процену ризика у информационо-комуникационим системима од посебног значаја („Сл. гласник РС“, бр. 63/2026), уз ослањање на међународно признате оквире за управљање ризиком информационе безбедности — ISO/IEC 27001 и ISO/IEC 27005 — и смернице америчког Националног института за стандарде и технологију (NIST Cybersecurity Framework). Мере заштите из чл. 10 ст. 4 Закона на којима се ова анализа ослања садржински одговарају мерама управљања сајбер ризиком из члана 21. Директиве (ЕУ) 2022/2555 (NIS2), чиме је обезбеђена усклађеност налаза са водећим европским и глобалним стандардима, независно од тога што Република Србија није чланица ЕУ.

Методологија процене ризика

За сваку претњу из Каталога претњи информационе безбедности израчуната је вероватноћа (на основу одговора клијента о постојећим мерама заштите) и утицај (на основу критичности погођених информационих добара из регистра ресурса), према формули Вредност ризика = Вероватноћа × Утицај (опсег 1–25). Налази у наставку груписани су у 12 тематских области ради прегледности руководству; комплетан регистар по појединачним претњама, GAP мапа усклађености са чл. 10 Закона и ставке за проверу дати су у прилогу.

Нивои ризика

Ниво	Значење
веома низак	Занемарљив утицај на пословање; постојеће мере су адекватне.
низак	Ограничен утицај; није приоритет за хитно деловање.
средњи	Умерена изложеност; потребне су корективне мере у разумном року.
висок	Значајна изложеност која може озбиљно угрозити податке или процесе; захтева приоритетно деловање.
веома висок	Критична изложеност која може довести до озбиљног прекида рада или трајног губитка података; захтева хитну интервенцију.

Налази по тематским областима

Управљање и организациона структура

Ниво ризика: веома висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] не постоје писана упутства за рад са кључним системима (§3.1), нити је јасно дефинисано ко је одговоран за поједине системе и процесе (§3.5). Додатно, не постоји формално задужена особа или тим за информациону безбедност (§3.17), иако је [ИМЕ ОДГОВОРНОГ ЛИЦА] наведено као лице одговорно за надзор над информационом безбедношћу и за праћење усклађености са прописима. Организациона структура у области информационе безбедности није успостављена (тачка 1), нису обезбеђени довољни ресурси за ову функцију (тачка 5), а статус усвајања релевантних докумената је нејасан (тачка 36).

ПРЕТЊА:
Одсуство писаних упутстава и јасне поделе одговорности (§3.1, §3.5) значи да у случају инцидента или одсуства кључног запосленог нико неће знати како да поступи нити ко је надлежан да реагује, што директно угрожава континуитет рада писарнице, архиве и издавања уверења грађанима. Непостојање формално задуженог лица или тима за безбедност (§3.17), уз неуспостављену организациону структуру и недовољне ресурсе (тачке 1 и 5), доводи до тога да безбедносни ризици остају непрепознати и неуправљани све док се инцидент не догоди.

ПРЕПОРУКА:
Потребно је формално успоставити организациону структуру за информациону безбедност, укључујући именовање лица или тима задуженог за ову област, уз јасно дефинисање одговорности за сваки систем и процес (тачка 1). Треба обезбедити адекватне ресурсе — кадровске, временске и финансијске — за обављање ових послова (тачка 5). Неопходно је израдити и усвојити писана упутства за рад са кључним системима, као и разјаснити и формално усвојити сва релевантна документа из области безбедности (тачка 36).

УТИЦАЈ:
Уколико се стање не промени, постоји реална опасност од прекида у вођењу матичних књига, раду писарнице и архиве, издавању уверења и решења грађанима, као и у наплати локалних јавних прихода. Ово би довело до немогућности пружања услуга грађанима, угрожавања поверљивости личних података и нарушавања поверења јавности у рад [НАЗИВ ФИРМЕ], уз могуће правне и репутационе последице.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 1 (Организациона структура) — није испуњено; тачка 5 (Довољно ресурса) — није испуњено; тачка 36 (Усвајање докумената) — нејасно

Политике безбедности и класификација

Ниво ризика: веома висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] не постоји формална политика класификације информација

(орг_5), иако су неформално препозната два нивоа осетљивости података — интерно и поверљиво (клас_1), укључујући личне податке грађана из матичних књига, податке о корисницима социјалне заштите и кадровске податке запослених (клас_2). Одлуку о томе којој категорији податак припада доноси надлежно одељење према врсти предмета, без писаног правила или формалне документоване одлуке (клас_5), а не постоје ни разлике у правилима руковања (дељење, штампање, чување) између нивоа осетљивости (клас_3), нити визуелно обележавање докумената нивоом поверљивости (клас_4). Правила о томе како се осетљиви подаци смеју делити путем имејла или штампе су потпуно недефинисана (§3.9), што је оцењено као ризик веома високог нивоа.

ПРЕТЊА:
Одсуство формалне класификације и правила руковања значи да запослени самостално и недоследно процењују осетљивост података, без јасних смерница за дељење, штампање или чување, што повећава вероватноћу ненамерног откривања или неовлашћеног дељења личних и поверљивих података грађана (§3.9). Како се ради о подацима из матичних књига, социјалне заштите и кадровској евиденцији, последице евентуалног цурења директно погађају права и приватност грађана, уз изложеност институције прекршајној и репутационој одговорности.

ПРЕПОРУКА:
Потребно је донети формалну политику класификације информација која дефинише нивое осетљивости (најмање интерно и поверљиво, уз разматрање додатних категорија по потреби), као и јасна правила руковања за сваки ниво — дељење путем имејла, штампање и физичко чување докумената. Потребно је увести обавезно визуелно обележавање докумената и фајлова одговарајућом ознаком поверљивости, као и писано упутство којим се одређује ко и на основу којих критеријума доноси одлуку о класификацији податка, уз евидентирање те одлуке. Овим мерама се адресирају и неиспуњене тачке из чл. 10 Закона — тачка 8 (Класификација података) захтева успостављање формалног система класификације, док тачка 14 (Заштита од отицања података) захтева да се на основу класификације уведу контроле које спречавају неконтролисано дељење осетљивих података. За спровођење и праћење примене ових мера треба задужити [ИМЕ ОДГОВОРНОГ ЛИЦА].

УТИЦАЈ:
Материјализација овог ризика би директно угрозила поверљивост личних података грађана и поверење јавности у рад институције, а могла би да наруши и континуитет кључних процеса попут издавања уверења и решења, рада писарнице и архиве, чиме би се успорило или онемогућило пружање услуга грађанима. Додатно, непостојање документоване класификације и правила руковања отежава доказивање усклађености са прописима у случају надзора или инцидента.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 8 (Класификација података) — није испуњено; тачка 14 (Заштита од отицања података) — није испуњено

Управљање приступом и идентитетима

Ниво ризика: веома висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] управљање приступом и идентитетима није успостављено на задовољавајући начин. Додела приступа подацима на основу стварне потребе није дефинисана (§3.16), приступ подешавањима система није ограничен искључиво на овлашћене администраторе (§4.2), не користи се вишефакторска аутентикација за кључне системе (§4.3), а периодична провера и уклањање непотребних права приступа се не спроводи (§4.4). Додатно, не постоји контрола која спречава неовлашћену измену или откривање кључних података (§4.10/4.12), процедура за хитно одузимање приступа запосленом који напушта фирму или мења позицију није дефинисана (§6.1), а рад на даљину није адекватно заштићен VPN-ом или еквивалентном безбедном везом и мерама против неовлашћеног приступа (§4.21). Једини позитиван налаз је да су лозинке личне и дељење налога је забрањено (§4.7).

ПРЕТЊА:
Непостојање контроле над доделом и одузимањем приступа, у комбинацији са одсуством MFA и незаштићеним радом на даљину, ствара реалну могућност да неовлашћена лица, бивши запослени или компромитовани налози приступе осетљивим подацима грађана и системима за вођење матичних књига, писарнице, архиве и наплате јавних прихода. Посебно је критично што се права приступа не преиспитују нити хитно укидају при промени посла или одласку запосленог (§6.1), чиме непотребна или злоупотребљена овлашћења могу остати активна неограничено дуго.

ПРЕПОРУКА:
Потребно је успоставити формалну политику доделе приступа засновану на принципу нужног знања, уз ограничавање администраторских права искључиво на овлашћена лица и увођење MFA за приступ кључним системима. Треба дефинисати и применити процедуру за хитно одузимање приступа при промени позиције или престанку радног односа, успоставити периодичну ревизију додељених права, као и техничке мере за спречавање неовлашћене измене или откривања података и отицања података. Рад на даљину је неопходно обезбедити путем VPN-а или еквивалентног безбедног решења са енкриптованом комуникацијом. Ове мере директно адресирају неиспуњене, односно нејасне ставке чл. 10 Закона: тачка 3 (безбедност рада на даљину), тачка 6 (заштита при промени послова запослених), тачка 10 (ограничење приступа), тачка 11 (одобравање овлашћеног приступа), тачка 12 (одговорност корисника), тачка 14 (заштита од отицања података) и тачка 37 (мултифакторска аутентификација).

УТИЦАЈ:
Материјализација овог ризика би директно угрозила могућност издавања уверења и решења грађанима, рад писарнице и архиве, вођење матичних књига и наплату локалних јавних прихода, уз нарушавање поверљивости личних података грађана. Овакав инцидент би довео до прекида пружања услуга јавне управе, губитка поверења грађана и могућих законских последица због неусклађености са прописима о заштити података и информационој безбедности.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 3 (Безбедност рада на даљину) — није испуњено; тачка 6 (Заштита при промени послова запослених) — нејасно; тачка 10 (Ограничење приступа) — није испуњено; тачка 11 (Одобравање овлашћеног приступа) — није испуњено; тачка 12 (Одговорност корисника) — није испуњено; тачка 14 (Заштита од отицања података) — није испуњено; тачка 37 (Мултифакторска аутентификација) — није испуњено

Прихватљиво коришћење и свест запослених

Ниво ризика: висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] не постоји политика о дозвољеном коришћењу ИТ опреме и интернета (§4.5), а преносиви медијуми и USB портови се не контролишу нити скенирају пре употребе (§2.9). Запослени не пролазе обуку из информационе безбедности (§3.15), укључујући обуку за препознавање социјалног инжењеринга и фишинга (§4.19), нити постоји обука при запошљавању (обк_1) или периодична обука за постојеће запослене (обк_2) — досадашња пракса показује да се обука никада није спроводила. Иако је програм обуке оквирно дефинисан темама попут фишинга, заштите података о личности и пријаве инцидената (обк_3), не постоје симулације провере ефикасности (обк_5), евиденција о спроведеним обукама (обк_6), нити је јасно да ли руководство пролази исту обуку (обк_4). Додатно, тренутно нико у управи није формално задужен за организацију и праћење програма обуке (обк_7).

ПРЕТЊА:
Без политике прихватљивог коришћења и контроле преносивих медијума, запослени могу несвесно унети малвер у систем или изнети осетљиве податке без икакве формалне препреке или санкције. Одсуство обуке чини запослене лако рањивим на фишинг и социјални инжењеринг, што у комбинацији са непостојањем одговорног лица за ову област значи да се ризик системски не препознаје нити смањује. С обзиром да [НАЗИВ ФИРМЕ] обрађује личне податке грађана кроз матичне књиге, писарницу и наплату прихода, људски фактор постаје најслабија карика кроз коју нападач може остварити неовлашћен приступ.

ПРЕПОРУКА:

Потребно је донети и објавити политику о дозвољеном коришћењу ИТ опреме и интернета, увести техничку контролу и скенирање USB уређаја и преносивих медијума пре употребе, као и успоставити обавезан програм обуке из информационе безбедности за све нове и постојеће запослене, укључујући руководство. Обуку треба допунити периодичним тест-фишинг симулацијама, евидентирањем резултата као доказа усклађености и формалним именовањем лица одговорног за организацију и праћење програма обуке — предлаже се да ову одговорност преузме [ИМЕ ОДГОВОРНОГ ЛИЦА] у координацији са лицем задуженим за усклађеност. Овим би се адресирале недостајуће мере из чл. 10 Закона: тачка 4 (оспособљеност лица која користе систем), тачка 9 (заштита носача података) и тачка 12 (одговорност корисника).

УТИЦАЈ:
Материјализација овог ризика могла би довести до компромитовања личних података грађана и прекида кључних процеса попут издавања уверења, решења и вођења матичних књига. Последице укључују губитак поверења јавности, прекршајну и правну одговорност установе због неусклађености са законским мерама, као и оперативне застоје у пружању услуга грађанима услед безбедносног инцидента изазваног људском грешком.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 4 (Оспособљеност лица која користе систем) — није испуњено; тачка 9 (Заштита носача података) — није испуњено; тачка 12 (Одговорност корисника) — није испуњено

Техничка заштита мреже и система

Ниво ризика: веома висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] управљање изменама и системским процесима није формализовано — није дефинисана провера „другог пара очију" за критичне ИТ измене (§3.2), провера подешавања пре пуштања у рад (§3.4), редовно ажурирање софтвера и оперативних система (§3.10), тестирање измена пре примене на продукцији (§3.11), као ни праћење искоришћености капацитета система (§3.12). Мрежни саобраћај, VPN везе и пренос фајлова нису заштићени енкрипцијом (§4.8/4.9), не постоји заштита од DoS напада на онлајн услуге (§4.15), нису уведене специфичне мере против рансомвера попут непроменљивих копија и сегментације мреже (§4.18), а мрежни штампачи и скенери нису ажурирани нити заштићени лозинком (§4.20). Додатно, није разматран дугорочни ризик пробијања постојеће енкрипције будућим квантним рачунарством (§2.8). Позитивно је што је заштита од злонамерног софтвера успостављена на свим уређајима (§3.6/4.6), што представља основни, али недовољан ниво техничке заштите.

ПРЕТЊА:

Непостојање контроле измена, тестирања и ажурирања система (§3.2, §3.4, §3.10, §3.11, §3.12) оставља простор да неопажене грешке или пропусти доведу до пада система или безбедносних рупа које се дуго не откривају. Недостатак енкрипције мрежне комуникације (§4.8/4.9) и незаштићени мрежни уређаји (§4.20) повећавају ризик од пресретања и злоупотребе података, док одсуство заштите од DoS напада (§4.15) и мера против рансомвера (§4.18) озбиљно угрожава континуитет рада. С обзиром да се обрађују лични подаци грађана (матичне књиге, уверења, решења), реализација било које од ових претњи може довести до недоступности услуга, губитка или компромитације података, уз дугорочни ризик од застаревања криптографске заштите.

ПРЕПОРУКА:
Потребно је успоставити формалну процедуру управљања изменама која укључује независну проверу (принцип четири ока), обавезно тестирање у контролисаном окружењу пре продукције, редован распоред ажурирања система и софтвера, као и континуирано праћење искоришћености капацитета. Мрежну комуникацију, укључујући VPN и пренос фајлова, треба енкриптовати савременим протоколима, увести заштиту од DoS напада, имплементирати мере специфичне за рансомвер (непроменљиве резервне копије, сегментација мреже) и обезбедити ажурирање и лозинком заштитити све мрежне штампаче и скенере. Додатно, потребно је спровести анализу дугорочне отпорности коришћених криптографских алгоритама на развој квантног рачунарства и укључити је у план модернизације. Ове мере директно адресирају GAP листе из чл. 10 Закона: тачка 13 (криптографске контроле), тачка 16 (заштита од губитка), тачка 19 (праћење система), тачка 20 (ограничење приступа веб презентацијама), тачка 25 (заштита од злоупотребе слабости), тачка 26 (заштита при ревизорском тестирању), тачка 27 (заштита података у мрежама), тачка 28 (безбедност података у комуникацији), тачка 29 (захтеви током животног циклуса) и тачка 34 (превенција инцидената) — све наведене тачке захтевају јасно дефинисање политика и контрола које тренутно недостају или су нејасне.

УТИЦАЈ:
Материјализација ових ризика би директно онемогућила вођење матичних књига, рад писарнице и архиве, као и издавање уверења и решења грађанима, чиме би [НАЗИВ ФИРМЕ] престала да пружа основне јавне услуге. Додатно, компромитација мреже или губитак података довели би до угрожавања поверљивости личних података грађана и наплате локалних јавних прихода, са правним, репутационим и оперативним последицама за институцију.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 13 (Криптографске контроле) — нејасно; тачка 16 (Заштита од губитка) — није испуњено; тачка 19 (Праћење система) — нејасно; тачка 20 (Ограничење приступа веб презентацијама) — нејасно; тачка 25 (Заштита од злоупотребе слабости) — није испуњено; тачка 26 (Заштита при ревизорском тестирању) — није испуњено; тачка 27 (Заштита података у мрежама) — није испуњено; тачка 28

(Безбедност података у комуникацији) — није испуњено; тачка 29 (Захтеви током животног циклуса) — нејасно; тачка 34 (Превенција инцидената) — није испуњено

Управљање подацима и складиштењем

Ниво ризика: веома висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] резервне копије података се редовно израђују (§3.8), што представља основу за континуитет пословања. Међутим, низ кључних контрола није дефинисано: не постоји потврђена контрола верзија нити потврда пре трајних измена важних података (§3.7), нејасно је да ли су осетљиви подаци енкриптовани и да ли се тестира успешност обнављања резервних копија (§3.20/3.21), није утврђено да ли се тест подаци штите од употребе стварних личних података (§3.22), нити да ли се подаци неповратно бришу по истеку прописаног рока чувања (§3.23). Додатно, резервне копије нису заштићене од брисања са компромитованог налога, односно не постоје одвојене/оффлине копије (§4.11). У складу са овим налазима, из чл. 10 Закона неиспуњена је тачка 16 (Заштита од губитка), док су нејасне тачка 13 (Криптографске контроле), тачка 17 (Исправност средстава), тачка 24 (Интегритет софтвера), тачка 30 (Заштита тест података) и тачка 31 (Процедуре чувања и брисања).

ПРЕТЊА:
Одсуство контроле верзија и потврде измена отвара могућност неовлашћених или случајних трајних измена података у матичним књигама и евиденцијама без могућности откривања или враћања на претходно стање. Недостатак енкрипције осетљивих података, незаштићених тест података и недефинисаних процедура брисања повећава ризик од неовлашћеног приступа и цурења личних података грађана, док неодвојене резервне копије значе да би нападач са компромитованим налогом могао уништити и продукционе и резервне податке истовремено, чиме би се онемогућио опоравак система.

ПРЕПОРУКА:
Потребно је увести формалну контролу верзија и обавезу потврде (нпр. двостепено одобрење) пре трајних измена или брисања кључних података, уз успостављање редовног тестирања обнављања резервних копија и чување бар једне копије оффлине или на физички одвојеном медију ван досега продукционих налога. Потребно је дефинисати и применити енкрипцију осетљивих података у складу са тачком 13 чл. 10 Закона, успоставити поступак заштите или анонимизације тест података (тачка 30), као и писане процедуре чувања и неповратног брисања података по истеку законског или уговореног рока (тачка 31). Додатно је неопходно разјаснити и документовати стање исправности средстава за обраду података (тачка 17) и механизме за проверу интегритета софтвера (тачка 24), како би се затворио GAP по свим наведеним тачкама чл. 10 Закона.

УТИЦАЈ:

Имајући у виду да кључни процеси [НАЗИВ ФИРМЕ] (вођење матичних књига, рад писарнице и архиве, издавање уверења и решења, наплата локалних јавних прихода) зависе од поузданости и доступности података, материјализација овог ризика би директно угрозила могућност издавања докумената и пружања услуга грађанима. Додатно, компромитација или губитак података довели би до повреде поверљивости личних података грађана и нарушавања поверења у рад органа јавне управе, уз могуће правне и репутационе последице.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 13 (Криптографске контроле) — нејасно; тачка 16 (Заштита од губитка) — није испуњено; тачка 17 (Исправност средстава) — нејасно; тачка 24 (Интегритет софтвера) — нејасно; тачка 30 (Заштита тест података) — нејасно; тачка 31 (Процедуре чувања и брисања) — нејасно

Мониторинг и евиденције

Ниво ризика: веома висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] није дефинисан процес редовног чувања и провере евиденција (логова) о активностима у информационим системима (§3.3), нити постоји дефинисан механизам за уочавање неуобичајене активности или план за случај престанка рада кључног система (§3.18/3.19). Додатно, евиденције активности нису заштићене од измене или брисања од стране неовлашћених лица (§4.1). У складу са овим налазима, неиспуњене или нејасне остају мере из чл. 10 Закона које се односе на прикупљање података о претњама (тачка 2), праћење система (тачка 19), чување података о догађајима (тачка 23) и континуитет послова (тачка 35).

ПРЕТЊА:
Без поузданих и заштићених евиденција, неовлашћени приступ, злоупотреба или безбедносни инцидент могу проћи непримећени или се накнадно не могу реконструисати, чиме се губи могућност утврђивања одговорности и обима штете. Одсуство механизма за детекцију неуобичајене активности и плана континуитета рада значи да би престанак рада кључног система (нпр. система за вођење матичних књига или наплату јавних прихода) могао остати нерешен дужи период, без јасно дефинисаног поступка опоравка.

ПРЕПОРУКА:
Потребно је успоставити формалну политику чувања и редовне провере евиденција (логова), са јасно дефинисаним роковима чувања и одговорним лицима за анализу. Треба увести техничку заштиту логова од неовлашћене измене или брисања (нпр. контрола приступа, централизовано и непроменљиво складиштење), као и механизам за детекцију неуобичајених активности у системима. Неопходно је израдити план континуитета пословања за кључне системе (матичне књиге, писарница, наплата прихода), укључујући процедуре за случај престанка рада, уз

јасно дефинисање улоге [ИМЕ ОДГОВОРНОГ ЛИЦА] у надзору над спровођењем ових мера.

УТИЦАЈ:
Материјализација овог ризика директно би угрозила способност [НАЗИВ ФИРМЕ] да издаје уверења, решења и друге услуге грађанима, као и рад писарнице, архиве и наплате локалних јавних прихода. Немогућност реконструкције догађаја и одсуство плана континуитета продужили би трајање прекида рада и отежали утврђивање узрока инцидента, док би неовлашћен приступ личним подацима грађана довео до нарушавања поверљивости и губитка поверења јавности у рад органа.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 2 (Прикупљање података о претњама) — није испуњено; тачка 19 (Праћење система) — нејасно; тачка 23 (Чување података о догађајима) — није испуњено; тачка 35 (Континуитет послова) — није испуњено

„Cloud“ сервиси и спољни ИТ провајдери

Ниво ризика: веома висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] статус уговора са спољним провајдером који регулише обраду личних података је недефинисан (§5.7), што представља основни налаз у овој области. Поред тога, нејасан је статус процедура за рачунарство у клауду (тачка 18), процедура чувања и брисања података (тачка 31), заштите средстава доступних пружаоцима услуга (тачка 32) и одржавања уговореног нивоа услуге (тачка 33). Додатно, није испуњена оспособљеност лица која користе систем (тачка 4), заштита од отицања података (тачка 14), нити превенција инцидената (тачка 34).

ПРЕТЊА:
Без јасно дефинисаног уговора којим се регулише обрада личних података, [НАЗИВ ФИРМЕ] нема гаранције да провајдер примењује адекватне мере заштите, нити основ за утврђивање одговорности у случају инцидента или цурења података (§5.7). Комбиновано са нејасним процедурама за рад у клауд окружењу, чување и брисање података, заштиту ресурса код пружаоца и одржавање нивоа услуге, као и недостатком оспособљености корисника, контроле отицања података и превенције инцидената, ризик од неовлашћеног приступа или губитка личних података грађана је веома висок и тренутно суштински неконтролисан.

ПРЕПОРУКА:
Потребно је хитно закључити или ревидирати уговор са провајдером којим ће се прецизно регулисати обрада личних података, укључујући обавезе, одговорности и мере заштите (§5.7). Паралелно треба формализовати и писано дефинисати процедуре за рачунарство у клауду, чување и брисање података, заштиту средстава код пружаоца услуге и услове одржавања уговореног нивоа услуге (тачке 18, 31, 32,

33), уз успостављање програма оспособљавања запослених, мера за спречавање отицања података и плана превенције инцидената (тачке 4, 14, 34). Одговорност за спровођење и праћење ових мера треба доделити [ИМЕ ОДГОВОРНОГ ЛИЦА].

УТИЦАЈ:
Материјализација овог ризика директно би угрозила кључне процесе који зависе од спољних ИТ провајдера и „cloud“ услуга, укључујући вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. Последица би била онемогућавање пружања услуга грађанима, повреда поверљивости личних података и нарушавање поверења јавности у рад [НАЗИВ ФИРМЕ], уз могућу правну одговорност због нерегулисаног односа са провајдером.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 4 (Оспособљеност лица која користе систем) — није испуњено; тачка 14 (Заштита од отицања података) — није испуњено; тачка 18 (Процедуре за рачунарство у клауду) — нејасно; тачка 31 (Процедуре чувања и брисања) — нејасно; тачка 32 (Заштита средстава доступних пружаоцима) — нејасно; тачка 33 (Одржавање уговореног нивоа услуге) — нејасно; тачка 34 (Превенција инцидената) — није испуњено

Реаговање на инциденте и опоравак

Ниво ризика: веома висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] постоји дефинисана процедура за пријаву губитка или крађе опреме (§3.13), што представља једини успостављени елемент у овој области. Насупрот томе, улога замене за кључне ИТ позиције у случају одсуства није дефинисана (§3.14), не постоји план опоравка у случају велике природне непогоде (§1.4), нема резервне опреме нити плана за квар кључног хардвера/софтвера (§2.4), као ни резервне интернет/телеком везе у случају отказивања примарне (§2.5). У складу са тим, мере из чл. 10 Закона које се односе на заштиту од губитка (тачка 16) и континуитет послова (тачка 35) нису испуњене.

ПРЕТЊА:
Непостојање плана континуитета и опоравка значи да би инцидент изазван природном непогодом, кваром хардвера/софтвера или прекидом интернет везе довео до продуженог прекида рада ИКТ система без јасног пута опоравка (§1.4, §2.4, §2.5). Додатно, одсуство дефинисане замене за кључне ИТ улоге (§3.14) значи да би и планирано или непланирано одсуство једне особе могло потпуно да парализује способност реаговања на инцидент, чиме се ризик додатно увећава.

ПРЕПОРУКА:
Потребно је израдити и формализовати план континуитета пословања и план

опоравка од катастрофе који покрива сценарије природних непогода, квара кључне опреме и прекида телекомуникационе везе, укључујући дефинисање резервне опреме и алтернативног интернет/телеком провајдера (§1.4, §2.4, §2.5). Неопходно је именовати и документовати заменике за све кључне ИТ улоге, уз јасно дефинисане овлашћења и процедуре предаје дужности у случају одсуства (§3.14). Ове мере треба ускладити са захтевима чл. 10 тачка 16 (заштита од губитка) и тачка 35 (континуитет послова), уз редовно тестирање планова. Постојећу процедуру за пријаву губитка/крађе опреме (§3.13) треба задржати и по потреби интегрисати у шири план управљања инцидентима.

УТИЦАЈ:
С обзиром да кључни процеси — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплата локалних јавних прихода — директно зависе од расположивости ИКТ система, продужени прекид рада би онемогућио пружање услуга грађанима и угрозио поверљивост личних података. Недостатак плана опоравка и континуитета би такав прекид додатно продужио, повећавајући ризик од губитка поверења јавности и нарушавања законом прописаних рокова за издавање докумената.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 16 (Заштита од губитка) — није испуњено; тачка 35 (Континуитет послова) — није испуњено

Физичка безбедност

Ниво ризика: висок

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] просторије са опремом су опремљене системом за детекцију и гашење пожара (§1.1), заштићене су од продора воде (§1.2), климатизоване су и заштићене од влаге и прашине (§1.3), поседују резервно напајање (§2.2) и физички су обезбеђене бравама, алармом и видео надзором (§4.14/4.16/4.17). Међутим, температура и влажност у серверској просторији се не надгледају редовно (§2.1), а опрема није заштићена од електромагнетних сметњи одговарајућим уземљењем или размаком од извора сметњи (§2.3).

ПРЕТЊА:
Одсуство редовног надзора над микроклиматским условима (§2.1) и недовољна заштита од електромагнетних сметњи (§2.3) повећавају вероватноћу неопаженог прегревања, влаге или сметњи које могу довести до отказа или оштећења опреме на којој се ослањају кључни системи. Како се ради о сектору јавне управе, овакав инцидент би могао настати без правовременог упозорења, чиме се ризик од прекида рада битно повећава.

ПРЕПОРУКА:

Потребно је успоставити систем за континуирано надгледање температуре и влажности у серверској просторији, са аутоматским обавештавањем одговорног лица у случају одступања од дозвољених вредности, чиме би се отклонио налаз §2.1. Такође је потребно спровести проверу и унапређење заштите опреме од електромагнетних сметњи, укључујући проверу уземљења и физичког размака од извора сметњи, ради отклањања налаза §2.3. С тим у вези, неопходно је формализовати и документовати мере физичке заштите објеката (тачка 15 члана 10 Закона) и мере заштите од губитка (тачка 16 члана 10 Закона), које су тренутно оцењене као неиспуњене, како би се обезбедила усклађеност са законским захтевима.

УТИЦАЈ:
Материјализација овог ризика могла би довести до отказа опреме која подржава вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода. Ово би директно угрозило континуитет пружања услуга грађанима, доступност личних података и поверење у рад [НАЗИВ ФИРМЕ] као органа јавне управе.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 15 (Физичка заштита објеката) — није испуњено; тачка 16 (Заштита од губитка) — није испуњено

Однос са трећим странама

Ниво ризика: нема података

Стање: СТАЊЕ:
У [НАЗИВ ФИРМЕ] однос са трећим странама се управља неформално, ослањајући се на дугогодишњу сарадњу са добављачем софтвера и ИТ одржаваоцем, без писаног процеса провере или периодичне ревизије (тр_1). Безбедносне провере се не спроводе ни пре потписивања уговора (вст_1), ни током његовог трајања (тр_2), а поновна провера постојећих добављача се никада формално не врши (вст_4). Провера нових добављача је сведена на уговорне клаузуле о поверљивости (вст_2), док клаузуле о обавештавању о безбедносним инцидентима нису јасно уређене ни у постојећим уговорима (тр_3), ни у стандардним уговорима који се тек закључују (вст_3). Додатно, не постоји формална процедура за раскид сарадње која би обухватила опозив приступа и повраћај или брисање података (вст_5), нити се приступ добављача интерним системима ограничава на најмању потребну меру и временски период (вст_6). У складу са овим налазима, мера из члана 10 Закона која се односи на тачку 32 — заштита средстава доступних пружаоцима — оцењена је као нејасна.

ПРЕТЊА:
Одсуство формалних провера и уговорних обавеза према трећим странама значи да [НАЗИВ ФИРМЕ] нема контролу над безбедносним праксама добављача који имају приступ интерним системима и подацима. У случају безбедносног инцидента код

добављача, фирма можда неће бити благовремено обавештена нити ће моћи да предузме правовремене мере, док неконтролисан и неопозван приступ трећих страна повећава ризик од неовлашћеног приступа подацима грађана и интерним системима и након престанка сарадње.

ПРЕПОРУКА:
Потребно је успоставити формалну процедуру провере добављача пре потписивања уговора, као и периодичну поновну проверу постојећих сарадника, укључујући ИТ одржаваоца и добављача софтвера. Стандардне уговоре треба допунити јасним клаузулама о обавези обавештавања о безбедносним инцидентима у дефинисаном року, као и одредбама о заштити средстава и података доступних пружаоцима услуга (тачка 32 чл. 10 Закона). Потребно је дефинисати и спровести процедуру за раскид сарадње која обухвата опозив приступа, повраћај или брисање података, као и увести принцип ограничавања приступа добављача на најмању потребну меру и временски период.

УТИЦАЈ:
Имајући у виду да кључни процеси попут вођења матичних књига, рада писарнице и архиве, издавања уверења и решења грађанима и наплате локалних јавних прихода зависе од ИКТ система, безбедносни пропуст код треће стране могао би директно угрозити континуитет пружања ових услуга грађанима. Такав инцидент би такође довео у питање поверљивост личних података грађана које фирма обрађује, са последичним репутационим и правним последицама за [НАЗИВ ФИРМЕ].

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 32 (Заштита средстава доступних пружаоцима) — нејасно

Лиценцирање софтвера и легалност система

Ниво ризика: низак

Стање: СТАЊЕ:
Према одговору на упитник, [НАЗИВ ФИРМЕ] софтвер преузима искључиво из поузданих, званичних извора (§4.13), што представља основу за контролу порекла софтвера који се користи у системима. Упркос томе, мера из чл. 10 Закона под тачком 24 — интегритет софтвера — оцењена је као нејасна, што значи да не постоји потврђен поступак провере целовитости и неизмењености софтвера након преузимања и током његове употребе.

ПРЕТЊА:
Ризик се огледа у могућности да, и поред преузимања из званичних извора, накнадна измена, неовлашћено ажурирање или компромитација софтвера остану непримећени услед непостојања јасно дефинисаног механизма провере интегритета (тачка 24). Ово је посебно осетљиво у сектору јавне управе, где се софтвером обрађују лични подаци грађана и воде евиденције од правног значаја.

ПРЕПОРУКА:
Потребно је успоставити и формализовати поступак провере интегритета софтвера — на пример контролу дигиталних потписа, хасх вредности или других механизама верификације — пре инсталације и периодично током експлоатације, и тај поступак јасно описати у интерним актима. Препоручује се да [ИМЕ ОДГОВОРНОГ ЛИЦА], као лице задужено за праћење усклађености, иницира дефинисање ове процедуре и њено документовање како би тачка 24 из чл. 10 Закона била недвосмислено испуњена.

УТИЦАЈ:
Имајући у виду да кључни процеси попут вођења матичних књига, рада писарнице и архиве, издавања уверења и решења грађанима и наплате локалних јавних прихода зависе од ИКТ система, компромитован или непроверен софтвер могао би угрозити тачност и поузданост ових услуга, као и поверљивост личних података грађана. Иако је тренутни ниво ризика низак, нејасан статус мере интегритета софтвера оставља простор за неопажену деградацију безбедности система током времена.

Мере из чл. 10 ст. 4 Закона релевантне за ову област (види и Акт о безбедности): тачка 24 (Интегритет софтвера) — нејасно

Преглед нивоа ризика по областима

Тематска област	Ниво ризика
Управљање и организациона структура	веома висок
Политике безбедности и класификација	веома висок
Управљање приступом и идентитетима	веома висок
Прихватљиво коришћење и свест запослених	висок
Техничка заштита мреже и система	веома висок
Управљање подацима и складиштењем	веома висок
Мониторинг и евиденције	веома висок
„Cloud“ сервиси и спољни ИТ провајдери	веома висок
Реаговање на инциденте и опоравак	веома висок
Физичка безбедност	висок
Однос са трећим странама	нема података
Лиценцирање софтвера и легалност система	низак

Закључак

Спроведена анализа ризика информационе безбедности у [НАЗИВ ФИРМЕ] показује да институција послује у условима изузетно високе изложености безбедносним ризицима, при чему је чак девет од једанаест анализираних области оцењено нивоом веома високог ризика. Посебно забрињава што се ова оцена односи и на фундаменталне области као што су управљање и организациона структура, политике

безбедности, управљање приступом и идентитетима, техничка заштита мреже, управљање подацима, мониторинг, сарадња са спољним ИТ провајдерима и „cloud“ сервисима, као и способност реаговања на инциденте и опоравка. 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 — у потпуности зависе од ИКТ система, овакво стање представља директну претњу континуитету пружања услуга грађанима и заштити њихових личних података.

Једини светао изузетак у анализи јесте област лиценцирања софтвера и легалности система, која је оцењена ниским ризиком, што указује да институција у овом сегменту послује усклађено и да постоји основ за успостављање реда и у другим областима по истом моделу. Физичка безбедност и прихватљиво коришћење система уз свест запослених оцењени су високим, а не веома високим ризиком, што говори да постоји делимична основа заштите, али ни она није на задовољавајућем нивоу и захтева хитно унапређење.

Највећи приоритет за деловање односи се на области управљања и организационе структуре, политика безбедности и класификације, управљања приступом, техничке заштите система, управљања подацима, мониторинга, „cloud“ сервиса и реаговања на инциденте — јер недостаци у овим областима делују кумулативно и међусобно се појачавају. Без јасно успостављеног управљачког оквира и политика, тешко је обезбедити доследну примену техничких контрола, а без адекватног мониторинга и плана реаговања на инциденте, институција нема могућност да правовремено детектује нити санира безбедносни догађај, што у јавној управи, због осетљивости података грађана и законске обавезе континуитета услуга, носи посебно висок ризик по репутацију и правну усклађеност институције.

Имајући у виду обим и озбиљност утврђених ризика, препоручује се да руководство, уз директно укључење [ИМЕ ОДГОВОРНОГ ЛИЦА] као лица одговорног за надзор над информационом безбедношћу, хитно усвоји план корективних мера са јасно дефинисаним приоритетима, роковима и одговорностима, почев од успостављања управљачког оквира и политика безбедности као основе на којој се граде све остале контроле. Даље кораке треба засновати на принципу поступног затварања најкритичнијих ризика, уз редовно праћење напретка и поновну процену ризика након спроведених мера, како би се обезбедио континуитет кључних процеса и заштита података грађана које институција обрађује.

Анализу урадио: Биро за дигиталну безбедност д.о.о.

Датум израде: 08.11.2026.

Руководство Општина потврђује да је упознато са садржајем ове анализе ризика.

У _____, ____.____._____. године

М.П.

Овлашћено лице:

_____

Прилози

Прилог 1: Регистар ресурса

Категорија	Тип	Назив	Власник	Критичност
Хардвер	Сервери	Локални сервер за писарницу и матичну књигу	Информатичар управе	критична
Хардвер	Радне станице / рачунари	Радне станице у шалтер сали и одељењима	Запослени / информатичар	висока
Хардвер	Мрежна опрема (рутери, свичеви)	Мрежна опрема управе	Информатичар управе	средња
Хардвер	Штампачи / скенери / МФП уређаји	Мрежни штампачи у шалтер сали и архиви	Администрација	ниска
Информације	Подаци о личности клијената	Лични подаци грађана из матичних књига и предмета	Матична служба	критична
Информације	Подаци о личности запослених	Кадровски подаци запослених	Одељење за општу управу	висока
Информације	Финансијски подаци	Подаци о локалним јавним приходима и буџету	Одељење за финансије	висока
Информације	Уговори и правна	Уговори о јавним набавкама и	Правна служба	средња

	документација	општи акти		
Локације	Главна канцеларија	Зграда Општинске управе Мионица	Начелник општинске управе	критична
Локације	Пословна јединица / филијала	Месна канцеларија (рурално подручје)	Повереник месне канцеларије	средња
Локације	Серверска соба / дата центар	Серверска просторија у згради управе	Информатичар управе	критична
Софтвер	Систем за управљање документима	Софтвер за писарницу и архиву (е-Писарница)	Информатичар управе	критична
Софтвер	База података	Матична књига (електронска евиденција)	Матична служба	критична
Софтвер	Веб сајт / портал	Званични сајт општине и портал за е-услуге	Спољни добављач / информатичар	средња
Софтвер	Рачуноводствен и софтвер	Софтвер за локалну пореску администрацију и буџет	Одељење за финансије	висока
Треће стране	ИТ / „cloud“ провајдер	Хостинг провајдер сајта/портала	-	средња
Треће стране	Добављач опреме / софтвера	Добављач софтвера за писарницу и матичну књигу	-	критична
Треће стране	Консултант / спољни сарадник	Спољни ИТ сарадник	-	висока
Треће стране	Подизвођач	Агенција за обезбеђење зграде управе	-	ниска
Запослени	Руководство / менаџмент	Начелник општинске управе и руководиоци одељења	-	критична
Запослени	Запослени са приступом осетљивим подацима	Матичари и службеници писарнице	-	висока
Запослени	Општи корисници	Административн и службеници по	-	средња

		одељењима		
Запослени	Спољни сарадници / консултанти	Спољни ИТ сарадник / добављач софтвера	-	висока

Прилог 2: Регистар ризика (појединачне претње)

Шифра	Претња	Одговор	Вероватноћа	Утицај	Ризик	Ниво
§2.8	Да ли сте размотрили ризик да садашња енкрипција буде пробијена будућим (квантним) рачунарством?	недефиниса но	5	4	20	веом а висо к
§3.1	Да ли запослени имају писана упутства за рад са кључним системима?	недефиниса но	5	4	20	веом а висо к
§3.10	Да ли редовно ажурирате софтвер и оперативне системе?	недефиниса но	5	4	20	веом а висо к
§3.11	Да ли се измене прво тестирају пре примене на продукционом систему?	недефиниса но	5	4	20	веом а висо к
§3.12	Да ли се прати искоришћеност капацитета система (простор, меморија)?	недефиниса но	5	4	20	веом а висо к
§3.14	Постоји ли замена за кључне ИТ улоге у случају одсуства?	недефиниса но	5	4	20	веом а висо к
§3.16	Да ли се приступ подацима додељује само онима којима је заиста потребан?	недефиниса но	5	4	20	веом а висо к
§3.18/3.19	Имате ли начин да приметите	недефиниса но	5	4	20	веом а

	неуобичајену активност, и план за случај престанка рада кључног система?					висок
§3.2	Да ли постоји провера „другог пара очију“ за критичне ИТ измене?	недефинисано	5	4	20	веома висок
§3.20/3.21	Јесу ли осетљиви подаци енкриптовани, и да ли тестирате успешност обнављања резервних копија?	недефинисано	5	4	20	веома висок
§3.22	Да ли се за тестирање ИКТ система користе подаци без стварних личних/осетљивих података (или се такви тест подаци посебно заштите)?	недефинисано	5	4	20	веома висок
§3.23	Да ли се подаци неповратно бришу по истеку прописаног или уговореног рока чувања?	недефинисано	5	4	20	веома висок
§3.3	Да ли се евиденције (логови) о активностима редовно чувају и проверавају?	недефинисано	5	4	20	веома висок
§3.4	Да ли се подешавања система проверавају пре пуштања у рад?	недефинисано	5	4	20	веома висок
§3.5	Је ли јасно дефинисано ко је одговоран за сваки систем и процес?	недефинисано	5	4	20	веома висок
§3.7	Постоји ли	недефиниса	5	4	20	веом

	контрола верзија или потврда пре трајних измена важних података?	но				а висок
§3.9	Постоје ли правила о томе како се осетљиви подаци смеју делити (имејл, штампа)?	недефинисано	5	4	20	веома висок
§5.7	Је ли са провајдером потписан уговор који регулише обраду личних података?	недефинисано	5	4	20	веома висок
§6.1	Постоји ли процедура за хитно одузимање приступа запосленом који напушта фирму или мења позицију?	недефинисано	5	4	20	веома висок
§1.4	Да ли постоји план опоравка у случају велике природне непогоде (земљотрес, поплава)?	не	4	4	16	висок
§2.1	Да ли се температура и влажност у серверској просторији редовно надгледају?	не	4	4	16	висок
§2.3	Је ли опрема заштићена од електромагнетних сметњи (уземљење, размак од извора)?	не	4	4	16	висок
§2.4	Да ли имате резервну опрему или план за случај квара кључног хардвера/софтвер	не	4	4	16	висок

	а?					
§2.5	Да ли имате резервну интернет/телеком везу ако примарна откаже?	не	4	4	16	висок
§2.9	Да ли су USB портови и преносиви медијуми контролисани или скенирани пре употребе?	не	4	4	16	висок
§3.15	Пролазе ли запослени обуку из информационе безбедности?	не	4	4	16	висок
§3.17	Постоји ли особа или тим формално задужен за информациону безбедност?	не	4	4	16	висок
§4.1	Јесу ли евиденције активности заштићене од измене/брисања од стране неовлашћених лица?	не	4	4	16	висок
§4.10/4.12	Постоји ли контрола која спречава неовлашћену измену или откривање кључних података?	не	4	4	16	висок
§4.11	Јесу ли резервне копије заштићене од брисања чак и са компромитованог налога (оффлине/одвојене)?	не	4	4	16	висок
§4.15	Је ли ваш сајт/онлајн услуга заштићена од преоптерећења	не	4	4	16	висок

	великим бројем захтева (DoS)?					
§4.18	Имате ли мере специфично усмерене против рансомвер напада (непроменљиве копије, сегментација мреже)?	не	4	4	16	висок
§4.19	Јесу ли запослени обучени да препознају социјални инжењеринг (лажни позиви, фишинг)?	не	4	4	16	висок
§4.2	Је ли приступ подешавањима система ограничен само на овлашћене администраторе?	не	4	4	16	висок
§4.20	Јесу ли мрежни штампачи/скенер и ажурирани и заштићени лозинком?	не	4	4	16	висок
§4.21	Је ли рад на даљину заштићен (VPN или еквивалентна безбедна веза, енкриптована комуникација, мере против неовлашћеног приступа са удаљених/мобилних уређаја)?	не	4	4	16	висок
§4.3	Користите ли вишефакторску аутентикацију (MFA) за приступ кључним системима?	не	4	4	16	висок
§4.4	Проверава ли се периодично ко има која права	не	4	4	16	висок

	приступа, уз уклањање непотребних?					
§4.5	Постоји ли политика о дозвољеном коришћењу ИТ опреме и интернета?	не	4	4	16	висок
§4.8/4.9	Је ли мрежни саобраћај и комуникација (VPN, пренос фајлова) заштићена енкрипцијом?	не	4	4	16	висок
§1.1	Да ли имате систем за детекцију и гашење пожара у просторијама са опремом?	да	2	4	8	низак
§1.2	Да ли су те просторије заштићене од продора воде (поплава, цурење цеви)?	да	2	4	8	низак
§1.3	Да ли су просторије климатизоване и заштићене од прекомерне влаге/прашине?	да	2	4	8	низак
§2.2	Да ли имате резервно напајање (УПС, агрегат) за кључну опрему?	да	2	4	8	низак
§3.13	Постоји ли процедура за пријаву губитка или крађе опреме?	да	2	4	8	низак
§3.6/4.6	Да ли имате заштиту од злонамерног софтвера (антивирус и сл.) на свим уређајима?	да	2	4	8	низак

§3.8	Да ли редовно правите резервне копије података?	да	2	4	8	низак
§4.13	Преузима ли се софтвер искључиво из поузданих, званичних извора?	да	2	4	8	низак
§4.14/4.16/4.17	Јесу ли просторије са опремом физички обезбеђене (браве, аларм, видео надзор)?	да	2	4	8	низак
§4.7	Јесу ли лозинке личне, уз забрану дељења налога?	да	2	4	8	низак

Прилог 3: GAP анализа — усклађеност са чланом 10 Закона

#	Мера (чл. 10 ст. 4)	Статус	Доказ (шифре претњи)
1	Организациона структура	није испуњено	§3.5, §3.17
2	Прикупљање података о претњама	није испуњено	§usk_5, §tech_17
3	Безбедност рада на даљину	није испуњено	§4.21
4	Оспособљеност лица која користе систем	није испуњено	§3.15, §4.19
5	Довољно ресурса	није испуњено	§usk_8
6	Заштита при промени послова запослених	нејасно	§6.1
7	Идентификовање информационих добара	испуњено	§registar-resursa
8	Класификација података	није испуњено	§org_5
9	Заштита носача података	није испуњено	§2.9
10	Ограничење приступа	није испуњено	§3.16, §4.4, §4.10/4.12
11	Одобравање овлашћеног приступа	није испуњено	§4.2

12	Одговорност корисника	није испуњено	§4.5, §4.7
13	Криптографске контроле	нејасно	§2.8, §3.20/3.21
14	Заштита од отицања података	није испуњено	§3.9, §4.10/4.12
15	Физичка заштита објеката	није испуњено	§1.1, §1.2, §1.3, §2.1, §2.3, §4.14/4.16/4.17
16	Заштита од губитка	није испуњено	§2.2, §3.13, §3.20/3.21, §4.11, §4.18
17	Исправност средстава	нејасно	§2.7
18	Процедуре за рачунарство у клауду	нејасно	§5.1, §5.2, §5.3, §5.6
19	Праћење система	нејасно	§3.12, §3.18/3.19
20	Ограничење приступа веб презентацијама	нејасно	§tech_15
21	Заштита од злонамерног софтвера	испуњено	§3.6/4.6
22	Резервне копије података	испуњено	§3.8
23	Чување података о догађајима	није испуњено	§3.3, §4.1
24	Интегритет софтвера	нејасно	§3.7, §4.13
25	Заштита од злоупотребе слабости	није испуњено	§3.10, §4.20
26	Заштита при ревизорском тестирању	није испуњено	§tech_12
27	Заштита података у мрежама	није испуњено	§4.8/4.9
28	Безбедност података у комуникацији	није испуњено	§4.8/4.9
29	Захтеви током животног циклуса	нејасно	§3.2, §3.4, §3.11
30	Заштита тест података	нејасно	§3.22
31	Процедуре чувања и брисања	нејасно	§3.23, §5.4
32	Заштита средстава доступних	нејасно	§5.5/5.8, §5.7, §5.11

	пружаоцима		
33	Одржавање уговореног нивоа услуге	нејасно	§5.1
34	Превенција инцидената	није испуњено	§4.15, §4.18, §5.5/5.8
35	Континуитет послова	није испуњено	§1.4, §2.4, §2.5, §3.14, §3.18/3.19
36	Усвајање докумената	нејасно	§3.1
37	Мултифакторска аутентификација	није испуњено	§4.3

За проверу (одговор „Не знам“)

§2.7 — Да ли се редовно проверава исправност медијума за складиштење података?

§5.1 — Бисте ли могли да промените „cloud“ провајдера без великог поремећаја пословања?

§5.11 — Проверавате ли безбедносну поузданост добављача хардвера/софтвера пре увођења?

§5.2 — Знате ли јасно које безбедносне обавезе сноси ваша фирма, а које провајдер?

§5.3 — Има ли ваш „cloud“ провајдер независан безбедносни сертификат (нпр. ISO 27001)?

§5.4 — Знате ли како провајдер трајно брише податке по раскиду уговора?

§5.5/5.8 — Је ли уговором дефинисано поступање по захтеву државних органа и подршка у случају инцидента?

§5.6 — Знате ли у којој се земљи физички налазе ваши подаци код „cloud“ провајдера?