Политика класификације и управљања подацима — Општина

ПОВЕРЉИВО — документ фирме „Општина“ је припрема за Политика класификације и управљања подацима. Не дистрибуирати ван БДБ тима и овлашћених лица клијента.

Датум генерисања: 08.11.2026. 03:42

Документ је припремљен на основу одговора клијента у упитнику за ову услугу. Пре усвајања од стране руководства, садржај проверити, допунити и уредити.

1. Сврха и обим примене

Овај документ успоставља нивое осетљивости података и правила руковања подацима у [НАЗИВ ФИРМЕ], у складу са Законом о информационој безбедности ("Сл. гласник РС", бр. 91/2025). Документ се примењује на све податке које [НАЗИВ ФИРМЕ] обрађује у оквиру пословних процеса вођења матичних књига, рада писарнице и архиве, издавања уверења и решења грађанима и наплате локалних јавних прихода, без обзира на формат у коме се подаци чувају (папирни документ, електронски фајл, запис у информационом систему).

Документ обавезује све запослене, ангажована лица и спољне сараднике који у оквиру својих задатака долазе у контакт са подацима које [НАЗИВ ФИРМЕ] обрађује, независно од одељења у коме су распоређени.

2. Правила и мере

2.1. Нивои осетљивости података

У [НАЗИВ ФИРМЕ] се подаци класификују у два нивоа осетљивости:

- Интерно — подаци намењени искључиво интерној употреби унутар [НАЗИВ ФИРМЕ], који нису јавно доступни, али чије откривање не представља непосредну повреду права грађана.
- Поверљиво — подаци чије неовлашћено откривање, измена или губитак представља повреду права и интереса грађана или запослених. У ову категорију спадају најмање:
  - лични подаци грађана из матичних књига,
  - подаци о корисницима социјалне заштите,
  - кадровски подаци запослених.

2.2. Сврставање података у ниво осетљивости

Припадност податка нивоу осетљивости одређује се према врсти предмета и надлежном одељењу које податак обрађује. Одељење које води матичне књиге, одељење надлежно за социјалну заштиту и одељење надлежно за кадровске послове поступају са подацима из своје надлежности као са подацима нивоа Поверљиво. Сви остали подаци који не припадају наведеним категоријама, а нису јавно доступни, сматрају се подацима нивоа Интерно.

Надлежно одељење је дужно да у случају недоумице о припадности податка нивоу осетљивости затражи писано мишљење [КЛИЈЕНТ ДА ДОПУНИ: назив функције или тела надлежног за одлучивање о спорним случајевима класификације]. Одлука о класификацији у спорним случајевима документује се [КЛИЈЕНТ ДА ДОПУНИ: начин и место евидентирања одлуке о класификацији].

2.3. Обележавање података

Документи и фајлови који садрже податке нивоа Поверљиво морају бити визуелно обележени ознаком "ПОВЕРЉИВО" у заглављу документа, наслову фајла или на други јасно уочљив начин, у зависности од формата у коме се документ чува или размењује. Обележавање спроводи лице које креира или прима документ у оквиру надлежног одељења, у тренутку креирања или пријема документа.

2.4. Правила руковања подацима нивоа Поверљиво

За податке нивоа Поверљиво примењују се следећа правила:

- Дељење — подаци нивоа Поверљиво достављају се искључиво лицима и институцијама која имају законски основ или службену потребу за приступ тим подацима. Достављање се врши путем [КЛИЈЕНТ ДА ДОПУНИ: канал достављања - нпр. службена пошта, интерни систем за размену докумената, електронска пошта са додатном заштитом].
- Штампање — штампање докумената нивоа Поверљиво дозвољено је искључиво у обиму неопходном за извршење службеног задатка. Одштампани примерци не смеју се остављати без надзора на штампачу, радном столу или у заједничким просторијама.
- Чување — папирни документи нивоа Поверљиво чувају се у закључаним орманима или просторијама са ограниченим приступом. Електронски подаци нивоа Поверљиво чувају се у системима којима приступ имају искључиво запослени надлежног одељења, у складу са њиховим радним задацима.
- Уништавање — документи нивоа Поверљиво који више нису потребни уништавају се на начин који онемогућава реконструкцију садржаја, у складу са [КЛИЈЕНТ ДА ДОПУНИ: правила и рокови архивирања/уништавања документације].

2.5. Правила руковања подацима нивоа Интерно

Подаци нивоа Интерно доступни су запосленима у оквиру њихових редовних радних задатака и не деле се ван [НАЗИВ ФИРМЕ] без одобрења надлежног руководиоца одељења. Чувају се у оквиру интерних система и просторија [НАЗИВ ФИРМЕ], без посебних додатних мера физичке или техничке заштите изнад стандардних мера контроле приступа просторијама и системима.

3. Одговорности

Више руководство (лице одговорно за надзор над информационом безбедношћу) — одговорно је за усвајање овог документа, обезбеђивање ресурса за његову примену и разматрање спорних случајева класификације података.

Лице одговорно за праћење усклађености са прописима о информационој безбедности — одговорно је за праћење примене овог документа, покретање измена документа када се промене врсте података које [НАЗИВ ФИРМЕ] обрађује и извештавање вишег руководства о стању усклађености.

Руководиоци надлежних одељења (матичне књиге, социјална заштита, кадровска служба) — одговорни су за исправно сврставање података из своје надлежности у одговарајући ниво осетљивости, за обележавање докумената нивоа Поверљиво и за надзор над применом правила руковања у свом одељењу.

Сви запослени — одговорни су за поступање са подацима у складу са нивоом осетљивости коме податак припада, укључујући обележавање, чување, дељење и уништавање докумената у оквиру сопствених радних задатака.

4. Процедуре

4.1. Поступак при креирању или пријему документа

Запослени који креира или прими документ проверава да ли податак припада категорији Поверљиво на основу врсте предмета и надлежности одељења. Уколико податак припада категорији Поверљиво, запослени обележава документ ознаком "ПОВЕРЉИВО" пре даље обраде, чувања или прослеђивања.

4.2. Поступак у случају недоумице о класификацији

Када запослени није сигуран ком нивоу осетљивости податак припада, обраћа се руководиоцу надлежног одељења. Уколико ни руководилац одељења не може да донесе одлуку, предмет се прослеђује [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности

за коначну одлуку о спорној класификацији], чија се одлука евидентира у складу са тачком 2.2 овог документа.

4.3. Поступак у случају сумње на неовлашћено откривање или губитак података нивоа Поверљиво

Запослени који примети неовлашћено откривање, губитак или приступ подацима нивоа Поверљиво дужан је да одмах обавести руководиоца свог одељења и лице одговорно за праћење усклађености са прописима о информационој безбедности. Даљи поступак пријаве и ескалације инцидента спроводи се у складу са интерним документом којим се уређује управљање безбедносним инцидентима.

4.4. Периодична провера примене

Лице одговорно за праћење усклађености са прописима о информационој безбедности спроводи периодичну проверу примене правила класификације и руковања подацима у надлежним одељењима, са учесталошћу од [КЛИЈЕНТ ДА ДОПУНИ: учесталост периодичне провере], и о налазима извештава више руководство.

Овај документ ступа на снагу даном усвајања од стране руководства Општина.

У _____, ____.____._____. године

М.П.

Овлашћено лице:

_____