Политика управљања приступом — Општина

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

Датум генерисања: 08.11.2026. 03:41

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 уређује начин додељивања, ревизије и одузимања приступа информационим системима и подацима у [НАЗИВ ФИРМЕ]. Документ се примењује на све запослене, ангажована лица по другом правном основу и спољне сараднике којима је потребан приступ систему писарнице, матичне књиге, као и другим информационим системима који се користе у раду [НАЗИВ ФИРМЕ], укључујући системе за издавање уверења и решења грађанима и систем за наплату локалних јавних прихода.

Обавезује сва организациона одељења која користе наведене системе, непосредне руководиоце одељења, информатичара управе, као и лице одговорно за праћење усклађености са прописима о информационој безбедности.

2. Правила и мере

Приступ системима додељује се искључиво на основу стварне потребе за обављање послова радног места. Обим овлашћења приступа мора одговарати опису послова запосленог, а не сме превазилазити оно што је неопходно за обављање конкретних радних задатака. [КЛИЈЕНТ ДА ДОПУНИ: начин на који се утврђује и документује обим неопходних овлашћења за свако радно место/систем].

Приступ систему писарнице и матичне књиге одобрава непосредни руководилац одељења, у договору са информатичаром управе. Сваки захтев за доделу приступа мора бити евидентиран у писаној форми (укључујући електронску пошту или други трајни запис), са назнаком система, обима овлашћења и образложењем потребе. [КЛИЈЕНТ ДА ДОПУНИ: образац или евиденција у којој се бележе одобрени захтеви за приступ].

Права приступа подлежу периодичној ревизији. Ревизија се спроводи најмање једном

годишње, а врши је непосредни руководилац одељења у сарадњи са информатичаром управе, ради провере да ли додељена овлашћења и даље одговарају тренутним пословним потребама запосленог. [КЛИЈЕНТ ДА ДОПУНИ: тачан рок и носилац одговорности за спровођење годишње ревизије, уколико се одступа од наведеног].

Приступ системима мора бити одузет по престанку радног односа или престанку потребе за приступом услед промене радног места. [КЛИЈЕНТ ДА ДОПУНИ: максималан рок за одузимање приступа по престанку радног односа, нпр. истог дана или у року од 24 часа].

Администраторски и други привилеговани налози (укључујући налоге информатичара управе) морају бити одвојени од стандардних корисничких налога истог лица, заштићени вишефакторском аутентификацијом и подложни логовању свих активности извршених под тим налогом. [КЛИЈЕНТ ДА ДОПУНИ: рок до ког ће бити успостављени посебни администраторски налози, MFA и систем логовања, с обзиром да тренутно не постоје].

3. Одговорности

Непосредни руководилац одељења одговоран је за подношење и одобравање захтева за доделу приступа запосленима у свом одељењу, као и за благовремено обавештавање информатичара управе о престанку потребе за приступом услед престанка радног односа или премештаја запосленог.

Информатичар управе одговоран је за техничко спровођење доделе, измене и одузимања приступа у системима, за вођење евиденције додељених овлашћења, за управљање привилегованим налозима и за спровођење логовања активности на тим налозима.

[ИМЕ ОДГОВОРНОГ ЛИЦА], као члан вишег менаџмента одговоран за надзор над информационом безбедношћу, одговоран је за надзор над спровођењем ове политике, одобравање њених измена и ескалацију у случајевима када ревизија приступа укаже на неусклађеност.

[ИМЕ ОДГОВОРНОГ ЛИЦА], као лице одговорно за праћење усклађености са прописима о информационој безбедности, одговорно је за праћење спровођења годишње ревизије права приступа, вођење доказа о спроведеним ревизијама и извештавање вишег менаџмента о утврђеним одступањима.

4. Процедуре

Додела приступа: Запослени или његов непосредни руководилац подноси захтев за приступ систему, са назнаком система и потребног обима овлашћења. Непосредни

руководилац одељења одобрава захтев и прослеђује га информатичару управе, који технички додељује приступ и евидентира доделу.

Ревизија приступа: Једном годишње, непосредни руководилац одељења у сарадњи са информатичаром управе проверава списак запослених са додељеним приступом и њихов обим овлашћења за сваки систем. Овлашћења која више нису неопходна морају бити укинута у оквиру исте ревизије. Резултати ревизије достављају се лицу одговорном за праћење усклађености са прописима о информационој безбедности.

Одузимање приступа: По престанку радног односа или премештају запосленог на друго радно место, непосредни руководилац одељења обавештава информатичара управе, који одузима сав приступ који више није потребан. [КЛИЈЕНТ ДА ДОПУНИ: рок у ком информатичар управе мора спровести одузимање приступа од тренутка пријема обавештења].

Управљање привилегованим налозима: Додела администраторског налога одобрава се посебно, одвојено од стандардног корисничког налога, уз обавезно успостављање вишефакторске аутентификације и активирање логовања активности. [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности за периодичну проверу записа о активностима администраторских налога].

Ескалација неправилности: Уколико се током ревизије или на други начин утврди да је приступ додељен супротно овој политици или да није благовремено одузет, информатичар управе обавештава непосредног руководиоца одељења и лице одговорно за праћење усклађености са прописима о информационој безбедности, које одлучује о даљим корацима и, по потреби, извештава [ИМЕ ОДГОВОРНОГ ЛИЦА].

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

У _____, ____.____._____. године

М.П.

Овлашћено лице:

_____