Политика управљања лозинкама — Општина

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

Датум генерисања: 08.11.2026. 03:39

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 утврђује правила за креирање, чување, промену и заштиту лозинки, као и за употребу мултифакторске аутентикације (MFA) у оквиру [НАЗИВ ФИРМЕ]. Документ обавезује све запослене, ангажоване спољне сараднике и друга лица која имају приступ информационим системима [НАЗИВ ФИРМЕ], укључујући системе за вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода, као и на све налоге путем којих се тим системима приступа, укључујући корисничке и сервисне/системске налоге.

2. Правила и мере

2.1. Лозинка мора имати најмање 8 карактера.

2.2. [КЛИЈЕНТ ДА ДОПУНИ: да ли лозинка мора садржати комбинацију великих и малих слова, бројева и специјалних знакова, или само део ових захтева]. До доношења ове одлуке, запослени су дужни да креирају лозинке које није могуће лако погодити и које не представљају уобичајене речи или низове карактера (нпр. "12345678", "лозинка").

2.3. Периодична промена лозинке се не захтева. Лозинка се обавезно мења у следећим случајевима: по сумњи или сазнању да је лозинка компромитована, након безбедносног инцидента који је могао утицати на налог, и при првом пријављивању на новоодобрен налог уколико је иницијална лозинка додељена од стране администратора система.

2.4. Коришћење менаџера лозинки није обавезно нити прописано овим документом.

2.5. Мултифакторска аутентикација (MFA) није обавезна ни за један систем у оквиру [НАЗИВ ФИРМЕ] у овом тренутку. [КЛИЈЕНТ ДА ДОПУНИ: да ли се планира увођење

MFA за системе који обрађују личне податке грађана или за приступ серверу, и у ком року].

2.6. Дељење корисничких налога и лозинки између запослених је изричито забрањено. Сваки запослени одговоран је за чување поверљивости сопствених приступних података и не сме их саопштавати другим запосленима, спољним сарадницима нити трећим лицима.

2.7. Сервисни/системски налози подлежу посебним правилима утврђеним у тачки 2.8, изузетно од опште забране дељења налога из тачке 2.6, с обзиром на то да поједини сервисни налози по својој природи захтевају приступ више овлашћених лица.

2.8. Сервисни налог за приступ серверу који користе информатичар управе и спољни ИТ сарадник мора имати евидентиране кориснике којима је приступ одобрен, а лозинка тог налога мора се мењати [КЛИЈЕНТ ДА ДОПУНИ: рок за промену лозинке сервисног налога, нпр. при свакој промени ангажовања спољног сарадника или периодично]. Приступ овом налогу ограничава се искључиво на лица наведена у овом документу или у интерној евиденцији приступа, а свака промена круга лица са приступом мора се евидентирати.

2.9. Безбедно ресетовање лозинке спроводи се искључиво након провере идентитета лица које захтева ресет, у складу са процедуром из дела 4 овог документа.

3. Одговорности

3.1. [ИМЕ ОДГОВОРНОГ ЛИЦА], као члан вишег менаџмента одговоран за надзор над информационом безбедношћу, одговоран је за усвајање и ревизију ове политике, као и за одлучивање о питањима из тачака 2.2 и 2.5 која су остављена на допуну.

3.2. [ИМЕ ОДГОВОРНОГ ЛИЦА], као лице одговорно за праћење усклађености са прописима о информационој безбедности, одговорно је за праћење примене ове политике, евидентирање изузетака (укључујући сервисни налог из тачке 2.8) и покретање поступка измене документа када се уочи неусклађеност.

3.3. Информатичар управе одговоран је за техничку администрацију налога, укључујући сервисни налог за приступ серверу, спровођење ресетовања лозинки по провери идентитета, и вођење евиденције лица којима је одобрен приступ сервисним налозима.

3.4. Спољни ИТ сарадник одговоран је за поштовање правила о чувању поверљивости лозинке сервисног налога за приступ серверу и за пријаву информатичару управе сваке сумње на компромитовање те лозинке.

3.5. Сваки запослени одговоран је за чување поверљивости сопствене лозинке, недељење налога са другим лицима и пријаву сумње на компромитовање своје лозинке информатичару управе.

4. Процедуре

4.1. Пријава сумње на компромитовану лозинку: Запослени који посумња да је његова лозинка или лозинка сервисног налога компромитована дужан је да одмах обавести информатичара управе. Информатичар управе спроводи хитну промену лозинке погођеног налога.

4.2. Ресетовање лозинке: Пре ресетовања лозинке било ког корисничког налога, информатичар управе спроводи проверу идентитета лица које захтев подноси. [КЛИЈЕНТ ДА ДОПУНИ: конкретан начин провере идентитета, нпр. лично присуство, провера преко службеног мејла или телефона, потврда непосредног руководиоца].

4.3. Одобравање и промена приступа сервисном налогу: Свака промена круга лица која имају приступ сервисном налогу за приступ серверу (нпр. промена спољног ИТ сарадника) мора бити праћена променом лозинке тог налога, о чему информатичар управе обавештава лице одговорно за праћење усклађености.

4.4. Ревизија политике: Лице одговорно за праћење усклађености са прописима о информационој безбедности спроводи периодичну проверу примене ове политике и предлаже [ИМЕ ОДГОВОРНОГ ЛИЦА] измене документа, нарочито у погледу захтева за сложеност лозинки и увођења MFA из тачака 2.2 и 2.5.

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

У _____, ____.____._____. године

М.П.

Овлашћено лице:

_____