Политика рада од куће — Општина

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

Датум генерисања: 08.11.2026. 03:38

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 услове и правила безбедног рада од куће у [НАЗИВ ФИРМЕ], укључујући коришћење опреме, приступ пословним системима и заштиту података ван просторија органа. Документ се примењује на све запослене којима је одобрен рад од куће, као и на сва лица која у том режиму приступају пословним системима, подацима или мрежи [НАЗИВ ФИРМЕ]. С обзиром на то да [НАЗИВ ФИРМЕ] обавља послове вођења матичних књига, рада писарнице и архиве, издавања уверења и решења грађанима и наплате локалних јавних прихода, рад од куће мора бити организован тако да се не угрози континуитет ових процеса нити поверљивост личних података грађана којима се у њима рукује.

2. Правила и мере

2.1. Рад од куће се одобрава повремено и искључиво на основу претходног договора са руководством. Без таквог одобрења запослени не сме приступати пословним системима ван просторија [НАЗИВ ФИРМЕ].

2.2. За рад од куће користи се комбинација пословне и личне опреме. Независно од власништва над уређајем, запослени који приступа пословним системима и подацима са личног уређаја дужан је да на њему примењује сва правила заштите прописана овим документом.

2.3. Приступ пословним системима од куће тренутно се остварује без обавезне VPN конекције или еквивалентне безбедне везе. [КЛИЈЕНТ ДА ДОПУНИ: да ли се уводи обавеза VPN приступа, од ког датума и за које системе, или се задржава директан приступ уз додатне мере].

2.4. Рад са јавних или незаштићених Wi-Фи мрежа (кафићи, аеродроми и сл.) није забрањен овим документом. [КЛИЈЕНТ ДА ДОПУНИ: да ли се уводи ограничење или забрана рада са оваквих мрежа, и под којим условима је дозвољен].

2.5. Уређаји коришћени за рад од куће морају имати активирано аутоматско

закључавање екрана и енкрипцију диска. [КЛИЈЕНТ ДА ДОПУНИ: рок до ког се ова мера спроводи на постојећим уређајима и лице задужено за проверу].

2.6. Пословни уређај који запослени користи за рад од куће не сме користити ниједан други члан домаћинства нити треће лице.

2.7. Сваки губитак или крађа уређаја коришћеног за рад од куће мора се пријавити без одлагања, у складу са процедуром из дела 4 овог документа.

2.8. Уређаји коришћени за рад од куће подлежу безбедносном надзору (антивирус/ЕДР агент, централизовано управљање) у мери у којој је то технички спроведено од стране [НАЗИВ ФИРМЕ]. [КЛИЈЕНТ ДА ДОПУНИ: рок и начин увођења централизованог надзора над уређајима који се користе за рад од куће].

2.9. Информатичар управе може повремено даљински приступати серверу ван редовног радног времена ради отклањања кварова. Сваки такав приступ мора бити евидентиран (датум, време, разлог интервенције). [КЛИЈЕНТ ДА ДОПУНИ: да ли се утврђује опште правило о доступности запослених током рада од куће, ван овог изузетка за информатичара].

3. Одговорности

Руководство [НАЗИВ ФИРМЕ] одобрава захтеве за рад од куће за сваки појединачни случај и процењује да ли су испуњени услови за безбедан приступ пословним системима.

[ИМЕ ОДГОВОРНОГ ЛИЦА], као лице одговорно за надзор над информационом безбедношћу, одговорно је за праћење примене овог документа и за одлучивање о мерама у случајевима безбедносних инцидената везаних за рад од куће.

[ИМЕ ОДГОВОРНОГ ЛИЦА], као лице задужено за праћење усклађености са прописима о информационој безбедности, одговорно је за периодичну проверу примене правила из овог документа и за предлагање измена у складу са променама прописа или уоченим недостацима.

Информатичар управе одговоран је за техничку подршку запосленима који раде од куће, укључујући подешавање безбедносних мера на уређајима (закључавање екрана, енкрипција, антивирус/ЕДР агент, када се уведу) и за евидентирање сопствених даљинских приступа серверу ван радног времена.

Сваки запослени који ради од куће одговоран је за безбедно чување уређаја и приступних података, за некоришћење пословног уређаја од стране других чланова домаћинства и за благовремену пријаву сваког безбедносног догађаја, укључујући

губитак или крађу уређаја.

4. Процедуре

4.1. Одобравање рада од куће
Запослени подноси захтев руководству пре почетка рада од куће, наводећи период и системе којима ће приступати. Руководство одобрава или одбија захтев, узимајући у обзир природу послова и осетљивост података којима запослени рукује.

4.2. Пријава губитка или крађе уређаја
Запослени је дужан да губитак или крађу уређаја коришћеног за рад од куће пријави [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности коме се пријава упућује] одмах по сазнању, а најкасније у року од [КЛИЈЕНТ ДА ДОПУНИ: рок за пријаву]. По пријему пријаве предузимају се мере заштите приступних података и пословних система којима је уређај имао приступ (промена лозинки, онемогућавање приступа, провера евиденције приступа).

4.3. Евидентирање даљинског приступа ван радног времена
Информатичар управе евидентира сваки даљински приступ серверу ван редовног радног времена, уз навођење датума, времена, разлога и предузетих радњи. Евиденција се доставља [ИМЕ ОДГОВОРНОГ ЛИЦА] на увид у оквиру периодичне провере усклађености.

4.4. Периодична провера примене
[ИМЕ ОДГОВОРНОГ ЛИЦА] спроводи периодичну проверу примене правила из овог документа, укључујући стање безбедносних подешавања на уређајима коришћеним за рад од куће, и о налазима извештава руководство [НАЗИВ ФИРМЕ]. [КЛИЈЕНТ ДА ДОПУНИ: учесталост провере].

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

У _____, ____.____._____. године

М.П.

Овлашћено лице:

_____