План реаговања на инциденте — Општина

ПОВЕРЉИВО — документ фирме „Општина“ је припрема за План реаговања на инциденте. Не дистрибуирати ван БДБ тима и овлашћених лица клијента.

Датум генерисања: 08.11.2026. 03:46

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 План реаговања на инциденте у [НАЗИВ ФИРМЕ] и примењује се на све запослене, ангажована лица и спољне сараднике који користе информационо-комуникационе системе фирме. План уређује поступање у случају безбедносног инцидента који погађа кључне пословне процесе — вођење матичних књига, рад писарнице и архиве, издавање уверења и решења грађанима и наплату локалних јавних прихода — као и инцидената који угрожавају поверљивост личних података грађана. План обухвата класификацију инцидената, обавештавање, пријаву Националном ЦЕРТ-у у законском року од 24 часа, интерну и спољну комуникацију, изолацију погођених система и анализу узрока након инцидента. План се примењује на све безбедносне инциденте, без обзира на то да ли су у потпуности спроведени или су на време спречени.

2. Правила и мере

2.1 Класификација инцидената

Сваки инцидент се класификује у један од следећа четири нивоа озбиљности: низак, средњи, висок и критичан. Критеријуми за разврставање инцидента у одговарајући ниво, укључујући процену утицаја на издавање докумената грађанима, поверљивост личних података и непрекидност рада писарнице и архиве, утврђује [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности за дефинисање критеријума класификације по нивоима озбиљности].

2.2 Типови инцидената који се посебно разматрају

План посебно разматра следеће типове инцидената: цурење или крађу података, компромитован кориснички налог и напад рансомвером. За сваки од ових типова инцидената примењују се општи кораци из овог плана (пријава, изолација, комуникација, анализа узрока), уз додатна упутства која утврђује [КЛИЈЕНТ ДА

ДОПУНИ: носилац одговорности за израду специфичних упутстава по типу инцидента].

2.3 Прва пријава инцидента

Свако лице које уочи безбедносни инцидент или сумњу на инцидент дужно је да о томе одмах обавести [ИМЕ ОДГОВОРНОГ ЛИЦА], које представља прву контакт особу за све инциденте, без обзира на ниво озбиљности.

2.4 Пријава Националном ЦЕРТ-у

Инциденти који подлежу законској обавези пријаве морају бити пријављени Националном ЦЕРТ-у најкасније у року од 24 часа од тренутка сазнања за инцидент. Пријаву ЦЕРТ-у спроводи [КЛИЈЕНТ ДА ДОПУНИ: лице или функција задужена за подношење пријаве ЦЕРТ-у], а садржај и начин подношења пријаве утврђује [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности за припрему садржаја пријаве]. Рок од 24 часа се рачуна од тренутка када је инцидент први пут уочен и пријављен првој контакт особи, у складу са тачком 2.3.

2.5 Комуникација са надлежним органима

[ИМЕ ОДГОВОРНОГ ЛИЦА] је једино лице овлашћено да комуницира са надлежним органима, укључујући ЦЕРТ и надлежну инспекцију, у вези са безбедносним инцидентима. Ниједно друго лице не сме самостално давати изјаве, податке или документацију овим органима без претходног одобрења овлашћеног лица.

2.6 Интерна комуникација током инцидента

Током трајања инцидента мора се обезбедити обавештавање руководилаца погођених организационих јединица и запослених који су неопходни за сузбијање инцидента. Носилац одговорности, редослед обавештавања и канал комуникације који се користи у току инцидента утврђује [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности за интерну комуникацију током инцидента, редослед и канал обавештавања].

2.7 Обавештавање грађана и корисника услуга

Уколико инцидент утиче на доступност услуга грађанима (издавање уверења и решења, рад писарнице, матичних књига или наплате локалних јавних прихода) или на поверљивост њихових личних података, грађани морају бити обавештени о привременој недоступности услуга или угрожавању њихових података. Услови под којима се обавештење издаје, рок у ком се објављује и канал обавештавања (нпр. огласна табла, интернет презентација, други вид јавног обавештења) утврђује

[КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности, рок и канал за обавештавање грађана о инциденту или недоступности услуга].

2.8 Изолација погођених система

Чим се инцидент уочи, погођени системи морају бити изоловани ради спречавања даљег ширења инцидента на друге системе, укључујући системе који подржавају рад писарнице, архиве и наплате јавних прихода. Поступак изолације, укључујући техничке кораке и лице задужено за њихово спровођење, утврђује [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности за спровођење изолације погођених система и конкретни технички кораци].

2.9 Резервни план рада у случају недоступности система

На основу претходног искуства са прекидом рада система за писарницу услед квара сервера, успоставља се обавеза да за кључне пословне процесе (писарница, архива, матичне књиге, наплата локалних јавних прихода) постоји резервни начин рада који омогућава наставак пружања услуга грађанима и током недоступности информационог система. Резервни начин рада и услове његове активације утврђује [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности за дефинисање резервног плана рада писарнице и других кључних процеса].

2.10 Анализа узрока након инцидента

Након сваког инцидента нивоа висок или критичан, спроводи се анализа узрока (пост-инцидент review) ради утврђивања узрока инцидента, ефикасности предузетих мера и потребних измена овог плана. Анализу спроводи [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности за спровођење анализе узрока и рок у ком се анализа спроводи након затварања инцидента].

2.11 Евиденција инцидената

Води се евиденција о свим безбедносним инцидентима, укључујући инциденте који су на време спречени или нису произвели штетне последице. Евиденција садржи најмање датум и време уочавања, ниво озбиљности, предузете мере и исход. Евиденцију води и ажурира [КЛИЈЕНТ ДА ДОПУНИ: носилац одговорности за вођење евиденције инцидената и место чувања евиденције].

3. Одговорности

Прва контакт особа ([ИМЕ ОДГОВОРНОГ ЛИЦА]) — прима пријаве инцидената од свих запослених, покреће поступак класификације инцидента и активира даље кораке из овог плана.

Овлашћено лице за комуникацију са надлежним органима ([ИМЕ ОДГОВОРНОГ ЛИЦА]) — искључиво оно комуницира са Националним ЦЕРТ-ом, инспекцијом и другим надлежним органима у вези са инцидентом.

Члан вишег руководства задужен за надзор над информационом безбедношћу ([ИМЕ ОДГОВОРНОГ ЛИЦА]) — надзире спровођење овог плана у целини, одобрава његове измене и одговоран је за усклађеност поступања фирме са законском обавезом пријаве инцидената ЦЕРТ-у.

Лице задужено за праћење усклађености са прописима о информационој безбедности ([ИМЕ ОДГОВОРНОГ ЛИЦА]) — прати да ли су рокови и процедуре из овог плана испоштовани у сваком конкретном случају инцидента и извештава више руководство о евентуалним одступањима.

Руководиоци организационих јединица (писарница, архива, матичне књиге, наплата јавних прихода) — обавештавају запослене у својој јединици о инциденту када је то релевантно и спроводе резервни начин рада из тачке 2.9 када се активира.

Сви запослени — дужни су да одмах пријаве уочени или сумњиви инцидент првој контакт особи и да поступају у складу са упутствима добијеним током трајања инцидента.

Формални тим за реаговање на инциденте (ИРТ) са дефинисаним улогама тренутно не постоји; до његовог евентуалног успостављања, улоге из овог плана обављају лица наведена у овој тачки.

4. Процедуре

4.1 Пријава инцидента
Корак 1: Лице које уочи инцидент одмах обавештава прву контакт особу ([ИМЕ ОДГОВОРНОГ ЛИЦА]).
Корак 2: Прва контакт особа класификује инцидент према нивоу озбиљности (низак, средњи, висок, критичан), у складу са тачком 2.1.
Корак 3: Прва контакт особа покреће поступак изолације погођених система, у складу са тачком 2.8.

4.2 Пријава ЦЕРТ-у и надлежним органима
Корак 1: Уколико инцидент подлеже законској обавези пријаве, пријава се подноси Националном ЦЕРТ-у најкасније у року од 24 часа од сазнања за инцидент, у складу са тачком 2.4.
Корак 2: Свака даља комуникација са ЦЕРТ-ом, инспекцијом или другим надлежним органом води се искључиво преко овлашћеног лица из тачке 2.5.

4.3 Интерна и спољна комуникација
Корак 1: Овлашћено лице покреће интерну комуникацију према руководиоцима погођених јединица и запосленима, у складу са тачком 2.6.
Корак 2: Уколико је погођена доступност услуга грађанима или поверљивост њихових података, покреће се обавештавање грађана у складу са тачком 2.7.
Корак 3: Уколико је погођен рад писарнице или другог кључног процеса, активира се резервни начин рада из тачке 2.9.

4.4 Анализа узрока и затварање инцидента
Корак 1: Након санације инцидента нивоа висок или критичан, спроводи се анализа узрока у складу са тачком 2.10.
Корак 2: Резултати анализе и предложене измене плана достављају се члану вишег руководства задуженом за надзор над информационом безбедношћу на одобрење.
Корак 3: Инцидент се евидентира у складу са тачком 2.11, без обзира на то да ли је довео до штетних последица.

4.5 Ревизија плана
Овај план се преиспитује након сваког инцидента нивоа висок или критичан, као и периодично, у роковима које утврђује [КЛИЈЕНТ ДА ДОПУНИ: рок периодичне ревизије плана и носилац одговорности за спровођење ревизије].

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

У _____, ____.____._____. године

М.П.

Овлашћено лице:

_____