

ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

Служба	Службени број	Датум	Период
400-735	2020-03/39		

БЕОГРАД
Макензијева 41

На основу члана 40. став 1. Закона о Државној ревизорској институцији („Службени гласник РС“ бр. 101/05, 54/07, 36/10 и 44/18) субјект ревизије, **Јавно комунално предузеће „Инфостан технологије“**, Данијелова 33, 11000 Београд, подноси

ИЗВЕШТАЈ О СПРОВОЂЕЊУ ПРЕПОРУКА РАДИ ОТКЛАЊАЊА НЕСВРСИСХОДНОСТИ
ОТКРИВЕНИХ У РЕВИЗИЈИ

„Управљање информационим системима у јавним предузећима за обједињену наплату ”

(тема ревизије)

Број и датум извештаја о ревизији: 400- 735/2020-03/26, Београд, 23. децембар 2020. године

Несврсисходности које су обухваћене налазима и закључцима, за које је у поступку ревизије утврђено да би њиховим отклањањем средства од стране субјекта ревизије била употребљена економичније, ефикасније и ефективније, као и у складу са планираним циљевима:

I

Несврсисходности које су обухваћене налазима приоритета 1, које је могуће отклонити у року од 90 дана.

1)

1.	Несврсисходност	<i>Иако је успостављен Регистар ризика нису обухваћени значајни ИТ ризици који могу изазвати поремећаје у пословању, делимичним, краткотрајним као и дужим прекидима у пружању услуга. То може довести до умањења поверења корисника у способност ЈКП да обављају додељене послове због којих су основани.</i>
2.	Опис мере исправљања	У оквиру израђење документације BCMS01.docx стратегије континуитета пословања и управљања кризним ситуацијама налази се прилог BCMS01.01.xlsx где су дефинисани регистри ризика по пословним процесима

3.	Докази који се прилажу уз овај извештај да је мера исправљања предузета	У прилогу се доставља документа BCMS01.01.xlsx где су дефинисани регистри ризика по пословним процесима
4.	Несврсисходност	Оснивач Град Београд није обавестио ЈКП које мере и активности за спречавање и умањење последица катастрофа треба да планира и шта се од ЈКП очекује у ванредним ситуацијама. ЈКП Инфостан технологије – Београд нема документован План континуитета пословања у ванредним ситуацијама, и досадашње поступање је одређено на основу стручне процене и искуства тренутно одговорних запослених лица.
5.	Опис мере исправљања	Препоручујемо ЈКП Инфостан технологије – Београд да покрене иницијативу код оснивача да им одреди потребне елементе у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама.
6.	Докази који се прилажу уз овај извештај да је мера исправљања предузета	ЈКП Инфостан Технологије је току припреме и достављања дописа оснивачу о покретању иницијативе за одређивање потребних елемената у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама
7.	Несврсисходност	Корисници информационог система нису редовно обавештавани нити обучавани како да препознају претње из сајбер простора.
8.	Опис мере исправљања	Препоручујемо ЈКП Инфостан технологије – Београд да успоставе процес обавештавања и обУ учавана запослених чија радна места су изложена сајбер нападима, планира и организује обучавање о новим обавезама која утичу на безбедност информационог система.
9.	Докази који се прилажу уз овај извештај да је мера исправљања предузета	Извршена је допуна је допуна постојећег документа „Правилник о безбедности информационо – комуникационог система ЈКП Инфостан технологије (члан 8.) а истим садржајем је планирана допуна постојећег SRPS ISO/IEC 27001:2014 – референтни циљеви контрола и контроле у делу А.7.7.2.2 упознавање са безбедношћу информација, образовање и обука где је дефинисан процес обавештавања и обучавања запослених у вези безбедности информационог система

Неврсисходности које су обухваћене налазима приоритета 2, које је могуће отклонити у року до годину дана.

РБ	Препорука	Мера исправљања	Функција или звање лица одговорног за предузимање мере исправљања	Период у којем се планира предузимање мере исправљања
1	<p>ЈКП Инфостан технологије – Београд да донесе План пословног континуитета са потребним елементима, именује тим за спровођење, увежбава, периодично га проверава и иновира</p>	<p>Извршена је израда документа ВСМС03 план континуитета пословања и опоравка од катастрофе у оквиру ВСМС01 стратегије континуитета пословања и управљања кризним ситуацијама, са свим потребним елементима где су такође дефинисана сва потребна тела за организацију пословања у кризним ситуацијама</p>	<p>Извршиће се формирање тимова за реакцију у кризним ситуацијама, сва потребна документација у вези пословног континуитета ће се периодично допуњавати и ажурирати</p>	<p>Током будућег пословања а у року не дужем од 12 месеца ће се извршити ресвалуација плана континуитета пословања и опоравка од катастрофе (BCP-DR) документ ВСМ03</p>
2	<p>ЈКП Инфостан технологије – Београд да изради Процену утицаја на пословање обухватајући све значајне пословне процесе, информационе системе и услуге, одреди очекивана времена и тачке опоравка за сваки ресурс као и смернице које мере применити.</p>	<p>Извршена је израда плана опоравка IS-a - документ ВСМС04 где је дефинисана и анализа утицаја на пословање. На основу података из ВСМС01.01 дефинисано је табела критични ресурси Друштва за подршку сервиса/пословних процеса су мапирани са IT ресурсима Друштва који представља VIA анализу IT процеса и сервиса за постојеће пословне процесе предузећа</p>	<p>У будућем периоду ће се у оквиру посебног пројекта извршити израда VIA за све пословне процесе предузећа</p>	<p>Овај пројекат за израду свеобухватног VIA за све службе у оквиру предузећа ће се реализовати у периоду не дужем од 24 месеци</p>

РБ	Препорука	Мера исправљања	Функција или звање лица одговорног за предузимање мере исправљања	Период у којем се планира предузимање мере исправљања
3	JKП Инфостан технологије – Београд да устави свеобухватни План опоравка од хаварије и врше његово редовно ажурирање.	У одговору на овај захтев извршена је израда плана опоравка IS-a - документ BCMS04 (у оквиру стратегије континуитета пословања и управљања кризним ситуацијама – документ BCMS01)	Током будућег пословања ће се дефинисати детаљне процедуре опоравка информационог система у оквиру плана опоравка IS-a документ BCMS04	Будуће планиране мере у року не дужем од 24 месеца
4	JKП Инфостан технологије – Београд да устави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организације обавештавање надлежног органа електронским путем.	У одговору на овај захтев извршена је допуна документа „Правилник о безбедности информационог система JKП Инфостан технологије (члана 32). У прилогу се налази документ „Proces upravljanja incidentima.docx“.	Извршиће се допуна одговарајућих контрола у оквиру постојећег SRPS ISO/IEC 27001:2014 – референтни циљеви контрола и контроле: A.16 менаџмент инцидентима нарушавања безбедности информација	У року не дужем од месец дана ће се извршити замена постојећег Правилника о безбедности информационог система JKП Инфостан Технологије који ће садржати наведене измене
5	JKП Инфостан технологије – Београд да устави редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник.	У одговору на овај захтев извршена је допуна документа „Правилник о безбедности информационог система JKП Инфостан технологије (члана 24). У прилогу се налази документ „Procedura pregleda log uređaja.docx“	Извршиће се допуна одговарајућих контрола у оквиру постојећег SRPS ISO/IEC 27001:2014 – референтни циљеви контрола и контроле: A.12.4.1 Записивање логова о догађајима	У року не дужем од месец дана ће се извршити замена постојећег Правилника о безбедности информационог система JKП Инфостан Технологије који ће садржати наведене измене

Докази који се прилажу уз овај извештај да ће мере исправљања бити предузете:

– нпр. акциони план...

Неврсисходности које су обухваћене налазима приоритета 3, које је могуће отклонити у року од једне до три године.

РБ	Препорука	Мера исправљања	Функција или звање лица одговорног за предузимање мере исправљања	Период у којем се планира предузимање мере исправљања
1	<p>ЈКП Инфостан технологије – Београд да обезбеди електронски начин двосмерног усавлашавања евиденција са предузећима пружаоцима услуга.</p>	<p>Извршена је имплементација размене података ESB-a (enterprise service bus) са циљем да обезбеди аутоматизовану и осигурану двосмерну размену података између ЈКП Инфостан Технологија и даваоца услуга. У овом тренутку систем се налази у тестној фази.</p>	<p>Планирана је даља разрада система размене података ESB-a (enterprise service bus) и проширење опсега на све даваоце услуга СОН-а.</p> <p>У оквиру овог успостављеног система размене података планира се прикључење свих спољних пословних корисника којима је неопходан овај сервис</p>	<p>у периоду не дужем од годину дана планира се успостављање ове размене података са свим даваоцима услуга</p>
2	<p>ЈКП Инфостан технологије – Београд да обезбеди механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације.</p>	<p>Овај захтев је планиран за имплементацију заједно са другим новим функционалностима система обраде података СОН-а.</p>	<p>Размотреће се сви доступни механизми којим би се остварила оваква врста заштите имајући у виду специфичност апликације за систем обједињене наплате.</p>	<p>Ова функционалност би се реализовала у периоду од наредне 3 године</p>

РБ	Препорука	Мера исправљања	Функција или звање лица одговорног за предузимање мере исправљања	Период у којем се планира предузимање мере исправљања
3	JKП Инфостан технологије – Београд да приликом израде извештаја омогуће избор датума последње измене из претходног извештајног периода.	Овај захтев је планиран за имплементацију заједно са другим новим функционалностима система обраде података будућег СОН-а. Због специфичности и начина прикупљања и обраде података у прошлости овај захтев представља изузетан проблем.	Разматра се нови систем за обједињену наплату који би поседовао овакву функционалност као саставни део стандардних могућности. У том контексту размотриће се начин приказа историјских података из претходне апликације СОН-а.	Ова функционалност би се реализовала у периоду од наредне 3 године
4	JKП Инфостан технологије – Београд да одреди линије за заштиту личних података и приступи изради Процену утицја обраде на заштиту личних података, а након тога изради план план имплементације псеудонимизације личних података корисника.	Овај захтев је планиран за имплементацију заједно са другим новим функционалностима система обраде података будућег СОН-а односно пратеће базе података.	У оквиру новог система за СОН би била знатно олакшана реализација овог захтева па ће се она извршити у току имплементације новог СОН-а.	Ова функционалност би се реализовала у периоду од наредне 3 године

Докази који се прилажу уз овај извештај да ће мере исправљања бити предузете:

– нпр. акциони план...

Докази о отклањању несврсиходности достављају се у прилогу извештаја.

Доказе о отклањању несврсиходности обухваћених налазима другог и трећег приоритета доставићемо након истека рока за предузимање мера.

ВД директора

