10789/2
28-05-2021

ЈКП „Информатика“ Нови Сад

Булевар цара Лазара 3, 21000 Нови Сад

ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

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, **ЈКП „Информатика“ Нови Сад, Булевар цара Лазара 3, 21000 Нови Сад,** 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	Дефинисање свих значајних ИТ ризика као и потребних елемената на основу којих се у складу са оцењеним утицајем на пословање може одредити адекватна мера у циљу избегавања или умањења негативног утицаја на пословање.
2.	Опис мере исправљања	У документу Процедура управљања ризицима дефинисана је методологија која се користи у процени и третману ризика у пословању ЈКП „Информатика“ Нови Сад с обзиром на поверљивост, интегритет и доступност информација које се налазе у дефинисаном подручју Система за управљање безбедношћу информација (ISMS), а према захтевима стандарда ISO/IEC 27001 и у складу са ISO/IEC 27005 – менаџмент ризицима по безбедност информација. Регистар ризика садржи све значајне ИТ ризике, процену ризика у складу са прописаном методологијом, постојеће мере и начин спровођења третмана ризика према захтевима стандарда ISO/IEC 27001.
3.	Докази који се прилажу уз овај извештај да је мера исправљања предузета	ЈКП „Информатика“ Нови Сад доставља документе: Процедура управљања ризицима Регистар ризика ЈКП „Информатика“ Нови Сад Листа мера безбедности Каталог претњи Каталог рањивости
4.	Несврсисходност	Покретање иницијативе да се одреде посебни елементи у оквиру Плана заштите и спасавања ради израде Плана за рад у ванредним ситуацијама
5.	Опис мере исправљања	ЈКП „Информатика“ Нови Сад израдила је План заштите и спасавања, који је предала Министарству унутрашњих послова, Одељењу за ванредне ситуације, како би добила сагласност на исти у сладу са Законом.
6.	Докази који се прилажу уз овај извештај да је мера исправљања предузета	ЈКП „Информатика“ Нови Сад доставља документе: Захтев за сагласност на План заштите и спасавања за ЈКП „Информатика“ Нови Сад План заштите и спасавања за ЈКП „Информатика“ Нови Сад
7.	Несврсисходност	Корисници информационог система нису редовно обавештавани нити обучавани како да препознају претње из сајбер простора.
8.	Опис мере исправљања	ЈКП „Информатика“ Нови Сад донела је посебан План екстерних и интерних обука запослених у вези са информационом безбедношћу, а Планом стручног усавршавања запослених (Q2.HR.02-2 ISO 27001:2013) обезбедила је и неопходна средства за њихову реализацију у 2021. години. Такође, ЈКП „Информатика“ Нови Сад организовала је и спровела за све запослене у марту и мају 2021. године две велике обуке у вези са Системом за управљање безбедношћу информација ISO 27001:2013 и подизањем свести о значају информационе безбедности за пословање предузећа. Обавештавање запослених регулисано је Процесом комуницирања екстерног и интерног ISO 27001:2013 и Упутством за запослене Q3.BI.01, а сви запослени на своје мејл адресе редовно добијају извештаје о претњама из сајбер простора (SOPHOS Quarantine Report). У овим извештајима наводе се све мејл адресе у карантину које су блокиране због нежељене поште, вируса, лоших екстензија датотека, забрањених израза или грешака у испоруци, а запослени су упућени да за сва питања обрате администратору поште.
9.	Докази који се прилажу уз овај	ЈКП „Информатика“ Нови Сад доставља документе:

	извештај да је мера исправљања предузета	План организовања екстерних и интерних обука у вези са безбедношћу информационог система за 2021. годину; План стручног усавршавања запослених Q2.HR.02-2 ISO 27001:2013 Презентација интерне обуке која је спроведена у марту месецу 2021. Презентација обуке запослених која је спроведена у мају месецу 2021. Евалуација интерне обуке запослених у вези са Системом за управљање безбедношћу информација ISO 27001:2013 (извештај) 03-05-1 Процес комуницирања екстерног и интерног ISO 27001:2013 Упутство за запослене Q3.BI.01 SOPHOS Quarantine Report Kaspersky Managed protection JKP Informatika

II

Несврсисходности 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	*ЈКП Информатика – Нови Сад 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.*	До дана достављања одазивног извештаја након ревидирања Регистра ризика реализована је Методологија управљања ризицима коју чине: •Идентификација ресурса и њихових власника •Идентификације вредности ресурса у односу на поверљивост, доступност и интегритет •Идентификације претњи •Идентификације рањивости •Вероватноћа појаве претњи који могу угрозити ове ресурсе •Оцењивање рањивости •Израчунавање укупног ризика •Идентификације власника ризика •Процена и третман ризика кроз одабир и примену мера безбедности	Разматрање мера које ће бити предузете у наредном периоду је у току	Именовани тим за увођење и развој ИСМС-а	У периоду од годину дана
2	*ЈКП Информатика – Нови Сад да успоставе свеобухватни План опоравка од хаварије и врше његово редовно ажурирање.*	Ревидирање процедуре План опоравка од хаварије је у току.	Након усвајања Плана опоравка од хаварије радиће се на његовом успостављању.	Именовани тим за увођење и развој ИСМС-а	У периоду од годину дана

РБ	Препорука	Мера исправљања		Функција или звање лица одговорног за предузимање мере исправљања	Период у којем се планира предузимање мере исправљања
3	*ЈКП Информатика – Нови Сад да успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организује обавештавање надлежног органа електронским путем.*	У току је ревизија постојеће Процедуре управљања инцидентима	Након усвајања Процедуре управљања инцидентима радиће се на њеној реализацији и примени	Именовани тим за увођење и развој ИСМС-а	У периоду од годину дана
4	*ЈКП Информатика – Нови Сад да успостави редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник.*	У току анализа тржишта и понуда везаних за Log Management Software	Спровести јавну набавку и имплементацију изабраног Log Management Software	Руководилац службе за информационо-комуникациону подршку	У периоду од годину дана

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

- *нпр. акциони план...*

Несврсисходности 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	*ЈКП Информатика – Нови Сад да обезбеди механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације.*	ЈКП „Информатика“ Нови Сад је започела активности на спровођењу ове препоруке.	ЈКП „Информатика“ Нови Сад је започела активности на спровођењу ове препоруке.	Именовани тим за увођење и развој ИСМС-а	У периоду од три године
2	*ЈКП Информатика – Нови Сад да одреди лице за заштиту личних података и приступи изради Процену утицаја обраде на заштиту личних података, а након тога изради план план имплементације псеудонимизације личних података корисника.*	ЈКП „Информатика“ Нови Сад је започела активности на спровођењу ове препоруке.	ЈКП „Информатика“ Нови Сад је започела активности на спровођењу ове препоруке.	Именовани тим за увођење и развој ИСМС-а	У периоду од три године

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

- *нпр. акциони план…*

Докази о отклањању несврсисходности достављају се у прилогу извештаја.

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

В. Д. директора

ЈКП „Информатика“ Нови Сад

Мр Гордана Стојсављевић