



ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

**ПОСЛЕРЕВИЗИОНИ ИЗВЕШТАЈ О МЕРАМА ИСПРАВЉАЊА
ЈАВНОГ ГРАДСКОГ САОБРАЋАЈНОГ ПРЕДУЗЕЋА НОВИ САД,
НОВИ САД**

**по ревизији сврсисходности пословања
„Информациони систем у јавном градском превозу у граду Новом Саду“**



**Број: 400-488/2023-07/51
Београд, 09. април 2024. године**



САДРЖАЈ

1. УВОД	3
2. НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА	4
2.1. Јавно градско саобраћајно предузеће Нови Сад није у потпуности успоставило организацију ИТ безбедности	4
2.1.1. Опис несврсисходности	4
2.1.2. Исказане мере исправљања и њихово вредновање (преорука 1)	4
2.2. Јавно градско саобраћајно предузеће Нови Сад није успоставило процес приступа систему на задовољавајући начин.	5
2.2.1. Опис несврсисходности	5
2.2.2. Исказане мере исправљања (преорука 2)	5
2.3. Јавно градско саобраћајно предузеће Нови Сад није успоставило план континуитета пословања у ванредним околностима	6
2.3.1. Опис несврсисходности	6
2.3.2. Исказане мере исправљања (преорука 3)	7
2.4. Јавно градско саобраћајно предузеће Нови Сад није успоставило управљање ИТ ризицима	8
2.4.1. Опис несврсисходности	8
2.4.2. Исказане мере исправљања (преорука 4)	8
2.5. Јавно градско саобраћајно предузеће Нови Сад није у потпуности процедурама и другим актима уредило сарадњу са пружаоцем услуга.	9
2.5.1. Опис несврсисходности	9
2.5.2. Исказане мере исправљања (преорука 6)	9
2.6. Јавно градско саобраћајно предузеће Нови Сад није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података	10
2.6.2. Исказане мере исправљања (преорука 8)	11
2.7. Јавно градско саобраћајно предузеће Нови Сад нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга	12
2.7.1. Опис несврсисходности	12
2.7.2. Исказане мере исправљања (преорука 10)	12
3. МИШЉЕЊЕ О ИСКАЗАНИМ МЕРАМА ИСПРАВЉАЊА	13



1. УВОД

Државна ревизорска институција издала је Извештај о ревизији сврсисходности пословања Информациони систем у јавном градском превозу у граду Новом Саду, број: 400- 488/2023-07/37, 25. децембар 2023. године, у којем је навела закључке и налазе.

С обзиром да, све откривене несврсисходности нису биле отклоњене у току ревизије, Институција је од субјекта ревизије, Јавног градског саобраћајног предузећа Нови Сад, захтевала достављање одазивног извештаја.

Субјект ревизије је у остављеном року од 90 дана доставио одазивни извештај потписан и оверен од стране одговорног лица 26. марта 2024. године. Документацију је доставио путем мејла 26. марта 2024. године.

У одазивном извештају су приказане мере исправљања утврђених несврсисходности. У послеревизионом поступку смо прегледали одазивни извештај, оценили његову веродостојност и оценили да ли су мере исправљања задовољавајуће.

У овом извештају:

- приказујемо несврсисходности које су обелодањене у извештају о ревизији за које је захтевано предузимање мера исправљања,
- резимирамо предузете мере исправљања и
- дајемо мишљење о томе да ли су мере за исправљање стања, исказане у одазивном извештају, задовољавајуће.



2. НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА

ПРИОРИТЕТ 2 - Несврсисходности које је могуће отклонити у року до годину дана

2.1. Јавно градско саобраћајно предузеће Нови Сад није у потпуности успоставило организацију ИТ безбедности

2.1.1. Опис несврсисходности

Организација ИТ безбедности у Јавном градском саобраћајном предузећу Нови Сад, због недостатка довољно стручног знања и недостатка кадровских капацитета, није успостављена тако да обухвата примену адекватних докумената која уређују ову област, управљање инцидентима и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система.

2.1.2. Исказане мере исправљања и њихово вредновање (преорука 1)

Јавном градском саобраћајном предузећу Нови Сад је препоручено да успостави организацију информационе безбедности која обухвата усвајање, ажурирање и имплементацију аката која уређују ову област – акта (правилника) о информационој безбедности, процедура које се односе на ИТ безбедност, управљање инцидентима, и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података.

Јавно градско саобраћајно предузеће Нови Сад је 21. марта 2024. године усвојило Акциони план и формирало Радну групу за поступање по препорукама Државне ревизорске институције, и као први циљ и активности за испуњење тог циља навело:

- Успоставити организацију информационе безбедности која обухвата усвајање, ажурирање и имплементацију аката која уређују ову област – акта (правилника) о информационој безбедности, процедура које се односе на ИТ безбедност, управљање инцидентима, и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података.

•Дефинисање политика информационе безбедности

•Ажурирање постојећег Акта о безбедности информационо-комуникационих система

•Ажурирање постојећих и креирање нових процедура за ИКТ безбедност, као што су:

-успостављање организационе ИКТ структуре

-безбедност рада на даљину и употреба мобилних уређаја

-контрола приступа

-заштита носача података

-физичка заштита

-заштита од злонамерног софтвера

-заштита од губитка података

-сарадња са пружаоцима услуга

-управљање инцидентима



-континуитет пословања

- Усвајање измењеног Акта о безбедности информационо-комуникационих система и пратећих процедура за ИКТ безбедност
- Имплементација Акта о безбедности информационо-комуникационих система и пратећих процедура за ИКТ безбедност
- Обезбедити адекватне ресурсе и алате за имплементацију
- Спровести дефинисане процедуре и политике у пракси
- Обука запослених за правилну имплементацију и поштовање новоусвојених аката

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији Број: 1864 од 22. марта 2024. године

Акциони план усвојен 21.03.2024. године

Решење о образовању и именовању радне групе за поступање по препорукама Државне ревизорске институције, број 1102 донето 20.02.2024. године

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.2. Јавно градско саобраћајно предузеће Нови Сад није успоставило процес приступа систему на задовољавајући начин.

2.2.1. Опис несврсисходности

У Јавном градском саобраћајном предузећу Нови Сад није успостављен процес приступа на задовољавајући начин, због тога што нису усвојене процедуре које уређују овај процес и није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података.

2.2.2. Исказане мере исправљања (препука 2)

Јавном градском саобраћајном предузећу Нови Сад је препоручено да уреди процес приступа систему, што подразумева усвајање процедура које уређују овај процес и контролу тог процеса, а односи се на логички приступ, рад на даљину и физичку заштиту система.

Јавно градско саобраћајно предузеће Нови Сад је 21. марта 2024. године усвојило Акциони план и формирало Радну групу за поступање по препорукама Државне ревизорске институције, и као први циљ и активности за испуњење тог циља навело:

Уредити процес приступа систему, што подразумева усвајање процедура које уређују овај процес и контролу тог процеса, а односи се на логички приступ, рад на даљину и физичку заштиту система.



- Утврђивање захтева за приступ систему
- Идентификовати категорије корисника и њихове потребе за приступом различитим ресурсима система
- Дефинисати минималне неопходне приступе за сваку улогу у организацији
- Разрада процедура за управљање логичким приступом, рад на даљину и физичку заштиту
- Креирати процедуре које уређују доделу, измену, и укидање приступних права
- Укључити политике за логички приступ (аутентификација, ауторизација), рад на даљину (VPN, двофакторска аутентификација) и физичку заштиту система (контрола приступа у просторије где се налазе сервери)
- Дефинисати систем за мониторинг и ревизију приступа
- Усвајање процедура за приступ систему
- Имплементација процедура за приступ систему
- Обука запослених о значају заштите приступа систему и обавезивање запослених на поштовање процедура

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији Број: 1864 од 22. марта 2024. године

Акциони план усвојен 21.03.2024. године

Решење о образовању и именовању радне групе за поступање по препорукама Државне ревизорске институције, број 1102 донето 20.02.2024. године

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.3. Јавно градско саобраћајно предузеће Нови Сад није успоставило план континуитета пословања у ванредним околностима

2.3.1. Опис несврсисходности

Јавно градско саобраћајно предузеће Нови Сад, због недовољно финансијских средстава па самим тим и недовољно хардверских ресурса, недовољно искуства и стручног знања и обученог ИТ кадра, није усвојила ни имплементирана правила и процедуре за континуитет пословања, иако је то и законска обавеза, а што може за последицу имати нефункционисање система у неодређеном временском периоду, па самим тим и отежано пружање услуга



2.3.2. Исказане мере исправљања (препорука 3)

Препоручујемо Јавном градском саобраћајном предузећу Нови Сад да успостави свеобухватан план континуитета пословања у ванредним околностима, што подразумева ажурирање постојећег Правилника о безбедности ИКТ система, усвајање процедуре за континуитет пословања у ванредним околностима и управљање резервним копијама података.

Јавно градско саобраћајно предузеће Нови Сад је 21. марта 2024. године усвојило Акциони план и формирало Радну групу за поступање по препорукама Државне ревизорске институције, и као први циљ и активности за испуњење тог циља навело:

- Успоставити свеобухватан план континуитета пословања у ванредним околностима, што подразумева ажурирање постојећег Правилника о безбедности ИКТ система, усвајање процедуре за континуитет пословања у ванредним околностима и управљање резервним копијама података.

•Детаљна анализа сегмената информационог система у погледу континуитета пословања, ради утврђивања оних аспеката код којих су захтеви за континуитет пословања испуњени, односно код којих постоји простор за побољшање. Елементи код којих су у одређеној мери већ обезбеђени ови захтеви:

-План опоравка после катастрофе за серверску инфраструктуру лоцирану у седишту ГСП-а која обезбеђује брзу реактивацију критичних система у случају непредвиђених догађаја

-За серверску (VMware) и мрежну (CISCO) инфраструктуру обезбеђена је континуирана подршка од стране произвођача, чиме се гарантује стабилност и поузданост система

-Дискови унутар система за складиштење података организовани су у RAID 1 (mirror) режиму: ако један диск откаже, систем може наставити да функционише користећи податке са другог диска, чиме се омогућава непрекидан рад, лака замена неисправног диска, као и висок ниво доступности и сигурности података

-Серверска инфраструктура је постављена на начин да подржава failover функционалност, омогућавајући да у случају кvara једног сервера други преузима његове функције без прекида у раду

-Сервер сале су опремљене уређајима за непрекидно напајање (UPS) и агрегатима, тако да је континуитет рада серверске инфраструктуре обезбеђен у случају прекида у снабдевању електричном енергијом

•Разрада детаљне процедуре за континуитет пословања која обухвата идентификацију критичних пословних функција и ресурса, анализу утицаја на пословање, стратегије опоравка и план дејства

•Одређивање улога и одговорности тимова и појединаца у случају активирања плана континуитета пословања

•Анализа стратегије резервних копија која укључује редовно прављење резервних копија свих критичних података, њихово складиштење на безбедним и географски одвојеним локацијама, и периодично тестирање опоравка података из резервних копија

•Анализа процедура за брз опоравак података и система из резервних копија у случају инцидента

•Усвајање плана за континуитет пословања



- Обука запослених о значају плана континуитета пословања и њиховим улогама и одговорностима у случају ванредних околности

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији Број: 1864 од 22. марта 2024. године

Акциони план усвојен 21.03.2024. године

Решење о образовању и именовању радне групе за поступање по препорукама Државне ревизорске институције, број 1102 донето 20.02.2024. године

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.4. Јавно градско саобраћајно предузеће Нови Сад није успоставило управљање ИТ ризицима

2.4.1. Опис несврсисходности

Јавно градско саобраћајно предузеће Нови Сад није успоставило управљање ИТ ризицима, што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера. Нарочито када се документација налази у електронском облику.

2.4.2. Исказане мере исправљања (препука 4)

Јавном градском саобраћајном предузећу Нови Сад је препоручено да успостави управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

Јавно градско саобраћајно предузеће Нови Сад је 21. марта 2024. године усвојило Акциони план и формирало Радну групу за поступање по препорукама Државне ревизорске институције, и као први циљ и активности за испуњење тог циља навело:

Успоставити управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика.

- Евидентирање и анализа постојећих ИТ ризика
- Развој стратегија за смањење или елиминацију ризика
- Периодична ревизија и ажурирање плана управљања ризицима

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији Број: 1864 од 22. марта 2024. године



Акциони план усвојен 21.03.2024. године

Решење о образовању и именовању радне групе за поступање по препорукама Државне ревизорске институције, број 1102 донето 20.02.2024. године

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.5. Јавно градско саобраћајно предузеће Нови Сад није у потпуности процедурама и другим актима уредило сарадњу са пружаоцем услуга

2.5.1. Опис несврсисходности

Јавно градско саобраћајно предузеће Нови Сад није у потпуности процедурама и другим актима уредило сарадњу са пружаоцем услуга, што за последицу има већи степен рањивости информационог система.

2.5.2. Исказане мере исправљања (препука 5)

Јавном градском саобраћајном предузећу Нови Сад је препоручено да усвоји/ажурира и имплементира правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера.

Јавно градско саобраћајно предузеће Нови Сад је 21. марта 2024. године усвојило Акциони план и формирало Радну групу за поступање по препорукама Државне ревизорске институције, и као први циљ и активности за испуњење тог циља навело:

Усвојити/ажурирати и имплементирати правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера

- Идентификација и анализа ризика у сарадњи са пружаоцима услуга

- Спровести детаљну анализу ризика који могу настати током обраде, преноса и складиштења података код пружаоца услуга

- Идентификовати критичне податке и процесе који захтевају посебне мере заштите

- Дефинисање правила и процедура које регулишу сарадњу са пружаоцима услуга, укључујући обавезне мере заштите података

- У процесу развоја и унапређења система потребно је предузети кораке ка дефинисању прецизних и детаљних захтева према добављачима и партнерима. Ови захтеви треба да обухватају широк спектар елемената неопходних за несметано и ефикасно функционисање целокупног система, укључујући, али не ограничавајући се на, гарантовање поузданости, доступности и скалабилности кључне хардверске инфраструктуре као што су централни и репликациони сервери, осигуравање високог нивоа сигурности и интегритета података, те имплементацију робусних процедура за одржавање и надзор система. Посебна пажња ће бити посвећена успостављању стандарда за редовно ажурирање, бекап и обнову података, као и за брзу реакцију у случају евентуалних техничких потешкоћа или прекида у раду. Добар део захтева је



начелно дефинисан уговорима са пружаоцима услуга али је потребно прецизирати у пракси временске оквире, одговорне особе, начине комуникације и обавештења, предуслове и одобрења за одређене активности пружаоца услуга и др.

-Оцена и одабир пружаоца услуга: приликом избора пружаоца услуга, неопходно је инсистирати на испуњавању релевантних безбедносних стандарда кроз поседовање одговарајућих сертификата, како би се осигурало да изабрани пружалац услуга задовољава високе захтеве у погледу заштите информација и интегритета система

- Усвајање правила и процедура за сарадњу са пружаоцима услуга

- Имплементација и мониторинг

-Имплементирати процедуре за редовно праћење и верификацију поштовања уговорених безбедносних мера од стране пружалаца услуга

-Успоставити механизме за брзо реаговање и управљање инцидентима који укључују безбедност података при сарадњи са пружаоцима

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији Број: 1864 од 22. марта 2024. године

Акциони план усвојен 21.03.2024. године

Решење о образовању и именовању радне групе за поступање по препорукама Државне ревизорске институције, број 1102 донето 20.02.2024. године

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.6. Јавно градско саобраћајно предузеће Нови Сад није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података

2.6.1. Опис несврсисходности

Јавно градско саобраћајно предузеће Нови Сад није у потпуности уредило сарадњу са пружаоцем услуга када је у питању заштита и обрада података, у смислу успостављања механизма којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да ли их спроводи, начина на који се прати реализација извршења уговора и на начин прописан Законом о информационој безбедности и Законом о заштити података о личности што за последицу има смањени степен поузданости система.



2.6.2. Исказане мере исправљања (препорука 6)

Јавном градском саобраћајном предузећу Нови Сад је препоручено да уреди сарадњу са пружаоцем услуга када је у питању заштита и обрада података, на начин прописан Законом о информационој безбедности и Законом о заштити података о личности.

Јавно градско саобраћајно предузеће Нови Сад је 21. марта 2024. године усвојило Акциони план и формирало Радну групу за поступање по препорукама Државне ревизорске институције, и као први циљ и активности за испуњење тог циља навело:

Уредити сарадњу са пружаоцем услуга када је у питању заштита и обрада података, на начин прописан Законом о информационој безбедности и Законом о заштити података о личности

- Анализа законских захтева

- Развој интерних политика и процедура

- Дефинисање уговора и споразума са пружаоцима услуга

- Укључити јасне и строге клаузуле о безбедности података у све уговоре са пружаоцима услуга, укључујући захтеве за примену конкретних безбедносних мера и одговорности у случају инцидената

- Предвидети механизме за праћење и верификацију примене ових мера.

- Усвајање правила и процедура за сарадњу са пружаоцима услуга

- Имплементација

- Потписивање одговарајућих уговора са свим пружаоцима услуга којима ће се дефинисати заштита података у складу са Законом о информационој безбедности

- Потписивање стандардних уговорних клаузула о заштити података о личности са пружаоцима услуга у складу са Законом о заштити података о личности

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији Број: 1864 од 22. марта 2024. године

Акциони план усвојен 21.03.2024. године

Решење о образовању и именовању радне групе за поступање по препорукама Државне ревизорске институције, број 1102 донето 20.02.2024. године

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.



2.7. Јавно градско саобраћајно предузеће Нови Сад нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга

2.7.1. Опис несврсисходности

Јавно градско саобраћајно предузеће Нови Сад нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга што за последицу може имати отежану продају карата, контролу персонализованих карата и онемогућено информисање грађана у дужем временском периоду.

2.7.2. Исказане мере исправљања (преорука 7)

Јавном градском саобраћајном предузећу Нови Сад је препоручено да успостави план континуитета пословања у случају раскида сарадње са пружаоцима услуга.

Јавно градско саобраћајно предузеће Нови Сад је 21. марта 2024. године усвојило Акциони план и формирало Радну групу за поступање по препорукама Државне ревизорске институције, и као први циљ и активности за испуњење тог циља навело:

Успоставити план континуитета пословања у случају раскида сарадње са пружаоцима услуга

- Разрада и усвајање процедура за континуитет пословања које укључују сценарије раскида сарадње са пружаоцима услуга (располагање подацима, начин употребе података након раскида уговора)
- Идентификација алтернативних пружалаца услуга и потенцијалних решења за прелазни период
- Имплементирање уговорне заштите кроз клаузуле о континуитету услуге и обавезама пружаоца после раскида уговора

Докази:

Извештај о спровођењу препорука ради отклањања несврсисходности откривених у ревизији Број: 1864 од 22. марта 2024. године

Акциони план усвојен 21.03.2024. године

Решење о образовању и именовању радне групе за поступање по препорукама Државне ревизорске институције, број 1102 донето 20.02.2024. године

Након истека рокова по датим приоритетима и достављања доказа оценићемо да ли су несврсисходности отклоњене. Отклањање утврђене несврсисходности је у току. Вредновање је извршено имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.



3. МИШЉЕЊЕ О ИСКАЗАНИМ МЕРАМА ИСПРАВЉАЊА

Прегледали смо одазивни извештај, који је поднео субјект ревизије. Оценили смо да је одазивни извештај, који је потписало и печатом оверило одговорно лице субјекта ревизије, веродостојан.

Вредновање мера исправљања смо оценили на основу њиховог описа и достављене документације (акционог плана субјекта ревизије којим су планиране активности на отклањању откривених неправилности/несврсисходности). Сматрамо да смо добили довољне и одговарајуће доказе да можемо изрећи мишљење да ли су мере исправљања задовољавајуће.

Оцењујемо, да су планиране мере исправљања, наведене у акционом плану и описане у одазивном извештају који је поднео Субјект ревизије задовољавајуће.

Напомена:

У складу са одредбама члана 37. Закона о Државној ревизорској институцији, потребно је да, до истека рока за спровођење препорука, обавештавате Државну ревизорску институцију о предузетим мерама и активностима на отклањању откривених несврсисходности и доставите одговарајуће доказе.

По истеку три године Државна ревизорска институција ће утврђивати ефекте остварене након спровођења препорука и отклањања откривених несврсисходности. У ове ефекте укључиће се и ефекти које сте исказали предузетим мерама и активностима из одазивног извештаја.

Генерални државни ревизор

Др Душко Пејовић

Државна ревизорска институција

Макензијева 41

11000 Београд, Србија

09. април 2024. године