ЈГСП „НОВИ САД“
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 ЈАВНО ГРАДСКО САОБРАЋАЈНО ПРЕДУЗЕЋЕ „НОВИ САД“, из Новиг Сада, Футошки пут 46 , подноси

ИЗВЕШТАЈ О СПРОВОЂЕЊУ ПРЕПОРУКА РАДИ ОТКЛАЊАЊА НЕСВРСИСХОДНОСТИ ОТКРИВЕНИХ У РЕВИЗИЈИ

Информациони систем у јавном градском превозу у граду Новом Саду (тема ревизије)

Број и датум извештаја о ревизији: 25.12.2023. 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, ЈАефикасније 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	*навести несврсисходност из извештаја о ревизији*
2.	Опис мере исправљања	*навести и описати мере и активности које су предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању*
3.	Докази који се прилажу уз овај извештај да је мера исправљања предузета	

…

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
	Навести препоруке из извештаја о ревизији	*навести и описати мере и активности које су предузете* до дана достављања одазивног извештаја *ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању*	*навести и описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању*	*навести које послове обавља или коју функцију врши лице које је одговорно за предузимање мере исправљања*	*навести када или у ком периоду ће бити предузета мера исправљања*
1	*Организација ИТ безбедности у организацији 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 (Препорука број 1).*		*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	Помоћница директора	10.4.2024. 10.5.2024. 10.6.2024.

			•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		20.06.2024. 01.08.2024. 02.09.2024
2	*У организацији процес приступа није успостављен 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 (Препорука број 2).*		*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	Шеф Одељења ИТ	15.05.2024. 02.09.2024 16.09.2024 01.10.2024 30.10.2024
3	*Организација није усвојила ни имплементирала правила и процедуре за континуитет пословања, иако је то и законска обавеза, што за последицу може имати нефункционисање система у неодређеном временском периоду, па самим тим и отежано пружање услуга (Препорука број 3).*		*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	Помоћница директора Шеф Одељења ИТ	 10.06.2024

			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 беспрекидан 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 квара 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		05.09.2024
			•Одређивање улога и одговорности тимова и појединаца у случају активирања плана континуитета пословања		05.09.2024
			•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		30.09.2024
			•Анализа процедура за брз опоравак података и система из резервних копија у случају инцидента		15.10.2024
			•Усвајање плана за континуитет пословања		01.11.2024
			•Обука запослених о значају плана континуитета пословања и њиховим улогама и одговорностима у случају ванредних околности		15.11.2024

4	*Организација није успоставила управљање ИТ ризицима, што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја који се могао спречити или великих нефинансијских губитака (нпр. података) због неблаговременог предузимања мера. Нарочито када се документација налази у електронском облику (Препорука број 4).*		*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	Помоћница директора Шеф Одељења ИТ	10.09.2024 20.10.2024
5	*Није успостављен ефективан механизам сарадње са пружаоцима услуга, зато што нису усвојена и имплементирана правила и процедуре када је у питању ова област, није обезбеђен континуитет пословања у случају раскида сарадње и процес обраде података о личности није уређен на начин прописан законом, организација није у потпуности процедурама и другим актима уредило сарадњу са пружаоцем услуга, што за последицу има већи степен рањивости информационог система (Препорука број 5).*		*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	Помоћница директора Шеф Одељења ИТ	26.08.2024. 26.09.2024.

			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		01.10.2024. 01.11.2024.
6	*Организација 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 их спроводи, као и 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 (Препорука број 6).*		*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	Помоћница директора	23.05.2024. 25.06.2024. 15.08.2024. 02.09.2024.

			•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		16.09.2024. 01.10.2024 01.11.2024
7	*Организација нема план континуитета пословања у случају раскида сарадње са пружаоцем услуга што за последицу може имати отежано одвијање пословних процеса и онемогућено информисање корисника у дужем временском периоду. (Препорука број 7).*		*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	Помоћница директора	16.08.2024 01.10.2024

			•Имплементирање уговорне заштите кроз клаузуле о континуитету услуге и обавезама пружаоца после раскида уговора		01.11.2024

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

- *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	*Навести препоруке из извештаја о ревизији*	*навести и описати мере и активности које су предузете* до дана достављања одазивног извештаја *ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању*	*навести и описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању*	*навести које послове обавља или коју функцију врши лице које је одговорно за предузимање мере исправљања*	*навести када или у ком периоду ће бити предузета мера исправљања*
2	...				
3					

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

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.

Помоћник директора

Леонтина Холо, дипл.маш.инг.

Holo Leontina

(потпис)