На основу члана 8. Закона о информационој безбедности (Службени гласник Р'С", број 6/16), чланова 1-8 Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, Владе РС ("Службени гласник РС", број 94/16 од 24.11.2016. године) и чл.23., а у вези са Статутом Јавног предузећа за подземну експоатацију угља Ресавица, директор Јавног предузећа за подземну експоатацију Ресавица угља доноси:

# АКТ О БЕЗБЕДНОСТИ

# ИНФОРМАЦИОНО - КОМУНИКАЦИОНИХ СИСТЕМА

# ЈППЕУ РЕСАВИЦА

## *I. Уводне одредбе*

Члан 1.

Овим Актом ближе се дефинишу мере заштите информационо-комуникационих система u Јавном предузеће за подземну експлоатацију угља Ресавица (у даљем тексту ЈППЕУ Ресавица), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса у ЈППЕУ Ресавица.

Члан 2.

Циљеви доношења овог Акта су:

- допринос подизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
- минимизација безбедносних инцидената;
- допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистентне контроле свих компонената информационо - комуникационог система (у даљем тексту: ИКТ систем).

Члан 3.

Овај Акт је обавезујући за све унутрашње организационе јединице ЈППЕУ Ресавица и за све кориснике информатичких ресурса, као и за сва трећа лица која користе информатичке ресурсе ЈППЕУ Ресавица. Непоштовање овог Акта повлачи дисциплинску одговорност корисника информатичких ресурса. За праћење примене овог Акта надлежни су Сектор за информационе технологије, Сектор за КОП и Финансијски сектор.

Члан 4.

Поједини појмови у смислу овог правилника имају следеће значење:

1) информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата:

a. електронске комуникационе мреже у смислу закона који уређује електронске комуникације;

b. уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;

c. податке који се похрањују, обрађују, претражују или преносе у сврху њиховог рада, употребе, заштите или одржавања;

d. организациону структуру путем које се управља ИКТ системом;

2) информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

3) тајност је својство које значи да податак није доступан неовлашћеним лицима;

4) интегритет значи очуваност изворног садржаја и комплетности податка;

5) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

7) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

8) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

9) управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

10) инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

11) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

12) информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

13)VPN (Virtual Private Network)-је „приватна“ комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;

14) Администратор ІКТ система – лице које има администраторски налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким

налогом, као и уношење и измену свих осталих корисничких налога.

15) Backup је резервна копија података;

16) ИТС – ИТ сектор је организациона јединица ЈППЕУ Ресавица чији је задатак управљање ИКТ система ЈППЕУ Ресавица сходно Акту о систематизацији радних места и послова

***II. Мере заштите***

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности ЈППЕУ Ресавица, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Интерни акти који уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу:

- Правилник о организацији и систематизацији радних места;
- Уговори о раду;
- Изјаве о поверљивости;
- Уговори о чувању поверљивости са правним лицима;

*1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у ЈППЕУ Ресавица*

Члан 6.

Сваки запослени-корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности.

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности појединих делова предузећа надлежни су:

РМU Рембас - Руководилац ИТ Сектора Рембас

РГП Алексинац - Водећи Администратор мреже

РМУ Боговина - Администратор мреже

РМУ Јасеновац – Администратор мреже

РКУ Ибарски Рудници - Инжењер за аутоматску обраду података и одрж. софтвера

РА Вршка Чука - Надзорник електро одржавања + администратор мреже

РМУ Штаваљ – Руководилац центра за АОП Штаваљ

РМУ Соко – Руководилац рачунског центра Соко

РЛ Лубница – Шеф електро службе + администратор мреже

Угаљпројект – Администратор мреже

За контролу и надзор свих надлежних за поједине делове предузећа, као и за безбедност целокупног ИКТ система ЈППЕУ Ресавица надлежан је Директор ИТ сектора ЈППЕУ Ресавица.

*2. Безбедност рада на даљину и употреба мобилних уређаја*

Члан 7.

Удаљени приступ се омогућава помоћу заштићене VPN конекције, преко које се корисници из појединих делова предузећа повезују на ИКТ систем ЈППЕУ Ресавице. Уређаји (VPN рутери) у истуреним деловима ЈППЕУ Ресавица (РА Вршка Чука, РКУ Ибарски рудници, РМУ Рембас, РМУ Боговина, РМУ Соко, РМУ Јасеновац, РМУ Штаваљ, РЛ Лубница, РГП Алексинац) морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем VPN мреже ИКТ система и уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера. Надлежни за поједине делове предузећа из члана 6. свакодневно контролише приступ ресурсима ИКТ система и проверава да ли има приступа са непознатих уређаја (са непознатих MAC адреса). Уколико се установи неовлашћен приступ о томе се путем електронске поште одмах, а најкасније сутрадан

обавештава Директор ИТ сектора, а та MAC адреса се уноси у «block“ листу софтвера који се користи за контролу приступа. Евиденцију приватних уређаја са којих ће бити омогућен приступ води надлежни за поједине делове предузећа из члана 6., а по одобрењу Директора ИТ сектора. Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране надлежних за поједине делове предузећа из члана 6. и могу се користити само за обављање послова у надлежности корисника-запосленог и то само у периоду када није могуће користити уређај у власништву ЈППЕУ Ресавица.

Употреба мобилних уређаја у ИКТ систему ЈППЕУ Ресавица није омогућен.

*3. Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност*

Члан 8.

Запослени у ИТ сектору који управљају ИКТ системом ЈППЕУ Ресавица се континуирано обучавају у циљу унапређења техничког знања. Надлежни за поједине делове предузећа из члана 6., су дужни  да сваког новозапосленог-корисника ИКТ ресурса упознају са одговорностима и правилима коришћења ИКТ ресурса ЈППЕУ Ресавица као и да воде евиденцију о изјавама новозапослених – корисника да су упознати са правилима коришћења ИКТ ресурса. Свако коришћење ИКТ ресурса ЈППЕУ Ресавица од стране запосленог-корисника, ван додељених овлашћење, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

*4. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система*

Члан 9.

У случају промене послова, односно надлежности корисника-запосленог, администратор система ће извршити промену привилегија које је корисник-запослени имао у складу са

описом радних задатака, а на основу захтева претпостављеног руководиоца. У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида. Корисник ИКТ ресурса, након престанка радног ангажовања у ЈППЕУ Ресавица, не сме да открива податке који су од значаја за информациону безбедност ИКТ система. Служба за опште и правне послове је у обавези да обавесте ИТ сектор о престанку радног ангажовања корисника-запосленог у року од три дана. Након тога ИТ сектор предузима следеће мере:

- Прегледа све налоге и приступе ИКТ систему који су били доступни кориснику
- Проверава све враћене рачунарске уређаје, уређаје за пренос података itd.
- Укида налог електронске поште и свих других права приступа ИКТ систему. Ова активност извршиће се у року од три дана од пријема одговарајућег обавештења

### *5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту*

Члан 10.

У информациона добра ЈППЕУ Ресавица спадају:

1) хардверске и софтверске компоненте ИКТ система;

2) подаци који се обрађују или чувају на информатичким ресурсима;

3) кориснички налози и други подаци о корисницима информатичких ресурса;

За евиденцију информационих добара појединих делова предузећа ЈППЕУ Ресавица, као и за њихову заштиту надлежни су извршиоци на радним местима из члана 6. овог акта.

*6. Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности*

Члан 11.

Подаци који се налазе у ИКТ систему представљају пословну тајну и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. Гласник РС“, бр. 53/2011).

*7. Заштита носача података*

Члан 12.

Подаци могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено одлуком Директора ИТ сектора ЈППЕУ Ресавица. Подаци и документи могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених – корисника. Евиденцију носача на којима су снимљени подаци води Руководилац одсека за информационе системе и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

*8. Ограничење приступа подацима и средствима за обраду података*

Члан 13.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има. Запослени који има администраторски налог, има права приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система. Запослени - корисник може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, сем администратору за подешавање корисничког профила и радне станице. Запослени-корисник који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности. Запослени-корисник дужан је

да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система, и то да:

1) користи информатичке ресурсе искључиво у пословне сврхе;

2) прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво ЈППЕУ Ресавица.

3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;

4) безбедно чува своје лозинке, односно да их не одаје другим лицима;

5) мења лозинке сагласно утврђеним правилима;

6) пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу

7) захтев за инсталацију софтвера или хардвера подноси у писменој или усменој форми, одобрен од стране непосредног руководиоца;

8) обезбеди сигурност података у складу са важећим прописима;

9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;

10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;

11) на радној станици не сме да складишти садржај који не служи у пословне сврхе;

12) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;

13) прихвати да технике сигурности (анти вирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему.

14) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

### *9. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа*

Члан 14.

Право приступа ИКТ систему имају само запослени/корисници који имају администраторске или корисничке налоге. Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога. Кориснички налог се састоји од корисничког имена и лозинке на основу којих се врши аутентификација – провера идентитета и ауторизација – провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника. Кориснички налог додељује администратор, на основу захтева запосленог задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем, а у складу са потребама обављања пословних задатака од стране запосленог-корисника. Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог на пословима управљања људским ресурсима, односно надлежног руководиоца.

### *10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију*

Члан 15.

Кориснички налог се састоји од корисничког имена и лозинке. Корисничко име се креира латиничним писмом без употребе следећих слова đ, ž , ć, č, dž, š. Уместо ових слова користе се dj,z,c,c,c,dz,s. Лозинка мора да садржи:

- најмање осам алфанумеричких карактера при чему у себи не смеју да садрже више од три узастопно иста бројна или словна знака.
- садржи комбинацију најмање три знака из следеће категорије:мало слово, велико слово, цифра и специјални знак.

Лозинке не смеју бити засноване на личним подацима особе, као што су име, презиме, телефонски број, датум рођења. Приликом креирања корисничког налога додељују се привремене лозинке које су корисници дужни да промене одмах након првог пријављивања. Ако запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени. Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

*11. Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података*

Члан 16.

У ЈППЕУ Ресавица није предвиђена употреба криптозаштите података.

*12. Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему*

Члан 17.

Простор у коме се налазе рачунари за вођење база података и централни рачунар (сервер), мрежна или комуникациона опрема ИКТ система, организује се као сервер соба. Сервер соба се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом. Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система. Осим администратора система, приступ сервер соби могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу

Директора ИТС-а. Сервер соба мора бити видљиво обележена и у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима. Прозори и врата на овој просторији морају увек бити затворени. Сервери и активна мрежна опрема (switch, modem, ruter, firewall ), морају стално бити прикључени на уређаје за непрекидно напајање – УПС. У случају нестанка електричне енергије, у периоду дужем од капацитета УПС-а, аутоматски се искључује опрема. У случају изношења опреме из просторије ради селидбе, или сервисирања, неопходно је одобрење Директора ИТС-а који ће одредити услове, начин и место изношења опреме. Ако се опрема износи ради сервисирања, поред одобрења Директора ИТС-а, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера. Уговором са сервисером обавезно се дефинише обавеза заштите података који се налазе на медијима који су део ИКТ ресурса ЈППЕУ Ресавица.

*13. Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем*

Члан 18.

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућности за неовлашћени приступ. Смернице за безбедност опреме:

- Опрема се поставља на месту који се може обезбедити од неовлашћеног приступа;
- Опрема за обраду информација која служи за приступ и коришћење осетљивих података се поставља не места која нису видљива особама које нису овлашћене;
- Просторије са опремом треба редовно чистити од прашине;
- Забрањено је конзумирање хране и пића и пушење близини опреме за обраду информација;
- Редовно се прате температура и влажност ваздуха;
- Опрема мора бити заштићена од атмосферских падавина;
- Опрема у индустријском окружењу се штити применом специјалних метода заштите.

Опрема се штити од прекида напајања, тако што се:

- помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
- капацитет помоћне опреме редовно процењује;
- редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова;
- обезбеђује вишеструко напајање са различитих траса.

Опрема се одржава како би се осигурали њена непрекидна расположивост и неповредивост, и то на следећи начин:

- опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;
- поправке и сервисирање опреме обавља само особље овлашћено за одржавање;
- о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;
- осетљиве информације треба избрисати из опреме;
- пре враћања опреме у рад након одржавања, треба је прегледати да би се уверили да није неовлашћено коришћена или оштећена.

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од прислушкивања, ометања или оштећења на следећи начин:

- водови напајања и телекомуникациони водови који улазе у просторије за обраду информација су подземни, онда када је то могуће, или имају адекватну алтернативну заштиту;
- каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње;
- за осетљиве или критичне системе се постављају оклопљени водови, користе закључане просторије или кутије, електромагнетско оклапање ради заштите каблова;
- неовлашћено прикључење уређаја на каблове се врши техничким претраживањем и физичком провером;
- приступ до разводних табли и у просторије са кабловима се контролише.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

*14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података*

Члан 19.

ЈППЕУ Ресавица ће усвојити радне процедуре које садрже инструкције за детаљно извршење следећих послова:

а) инсталација и конфигурација система;

б) обраду и поступање са информацијама (аутоматски и мануелно);

в) израда резервних копија;

г) захтеви за временски распоред активности;

д) инструкције за поступање према грешкама или другим ванредним стањима која могу да настану у току извршавања посла;

ђ) контакти за подршку (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;

е) инструкције за поступања према поверљивим подацима;

ж) процедуре за поновно покретање система и опоравак, које се користе у случају отказа система;

з) управљање информацијама о трагу провере система и системским записима (логовима);

и) процедуре за надгледање.

За усвајање, измене и допуне радних процедура овлашћен је Директор ИТС-а.

*15. Заштита података и средства за обраду података од злонамерног софтвера*

Члан 20.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, и-мејлом, зараженим преносним медијима (USB меморија, CD итд.), инсталацијом нелиценцираног софтвера и сл. За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. У циљу заштите ИКТ система од малициозног софтвера неопходна је примена: лиценцираног софтвера, односно забрана коришћења неауторизованог софтвера; Преносиви медији пре коришћења морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, врши се чишћење медија од вируса, уз сагласност доносиоца медија. Ризик од евентуалног губитка података приликом чишћења медија антивирусним софтвером, сноси доносилац медија. У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

• електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;

• забрањено је коришћење електонске поште у приватне сврхе; не смеју се користити приватни налози електронске поште у пословне сврхе.

16. Заштита од губитка података

Члан 21.

ЈППЕУ Ресавица врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.  Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују. Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера,

грешака корисника, природних катастрофа и других несрећа. Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

Заштита од губитка података у ЈППЕУ Ресавица се обезбеђује тако што се се једном дневно – ноћу аутоматски прави резервна копија свих података. Резервна копија свих података се чува 14 дана уназад на самом серверу, а такође се свакодневно врши пренос backup-а са сервера на мрежни диск. Једном месечно се резервне копије снимају на екстерни цд- носач, који се чува на за то предвиђеном и обезбеђеном месту. Исправност копија - архива проверава се најмање на шест месеци и то тако што се врши враћање база података које се налазе на медију, при чему подаци после враћања треба да буду исправни и спремни за употребу.

*17. Чување података о догађајима који могу бити од значаја за безбедност ИКТ система*

Члан 22.

О активностима администратора и запослених-корисника воде се дневници активности (activitylog, history, securitylog, transactionlog и др). Сваког последњег радног дана у месецу датотеке у којима се налази дневник активности се архивирају по процедури за израду копија-архива осталих података у ИКТ систему.

*18. Обезбеђивање интегритета софтвера и оперативних система*

Члан 23.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву ЈППЕУ Ресавица , односно Freeware и Opensource верзије. Инсталацију и подешавање софтвера може да врши само запослени-корисник који има овлашћење за то. Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера. Пре сваке инсталације нове верзије софтвера,

односно подешавања, неопходно је направити копију постојећег, како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

*19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система*

Члан 24.

ЈППЕУ Ресавица врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите. Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, запослени у ИТС-у је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости. Смернице које треба поштовати у циљу заштите од злоупотребе техничких безбедоносних слабости ИКт система:

- ЈППЕУ Ресавица дефинише и успоставља улоге и одговорности у вези са управљањем техничким рањивостима, укључујући надзор, оцену ризика услед утврђене рањивости, исправке, следљивост имовине и све одговорности за потребна координирања;
- најмање једном месечно а по потреби и чешће врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др ) у циљу идентификације потенцијалних слабости ИКТ система.
- за софтверске и друге технологије (засноване на списку имовине: видети 5.1) се одређују информациони ресурси за идентификовање одговарајућих техничких рањивости и за одржавање свести о истима;
- када је могућа техничка рањивост идентификована, тада се идентификују припадајући ризици и акције које треба предузети; такве акције могу да обухвате исправке рањивих система и/или примену других контрола;
- у зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, предузете активност се спроводе у складу са контролама које су

везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности;

- исправке се морају прво испробати и вредновати пре него што се трајно угради, како би се осигурало да ће оне бити ефективне и да неће довести до споредних утицаја који се не могу толерисати; ако исправка није на располагању, онда треба размотрити друге контроле, као што су деактивирање услуга или могућности које се односе на рањивост, прилагођавање или додавање контрола приступа, (нпр. заштитну баријеру на границама мреже или појачано надгледање како би се открили или спречили постојећи напади и утицало на повећање свести о рањивости;

*20. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система*

Члан 25.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника-запослених. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност Директора ЈППЕУ Ресавица.

*21. Заштита података у комуникационим мрежама укључујући уређаје и водове*

Члан 26.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења. Мрежна опрема (switch, router, firewall) се мора налазити у закључаном rack орману. Запослену и ИТС-у је дужан да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

*22. Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система*

Члан 27.

Заштита података који се преносе комуникационим средствима унутар ЈППЕУ Ресавица, између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

- Правила коришћења електронске поште

Електронска пошта се може користити искључиво за пословне потребе. Размена порука личног садржаја није дозвољена. Није дозвољено да се пословне е - mail адресе користе за регистровање на друштвеним мрежама и другим порталима (изузев порталима којима се приступа због потребе посла).

- Правила коришћења интернета

У циљу заштите, односно упада у ИКТ систем са интернета, надлежни субјект ИКТ система је дужан да одржава систем за спречавање упада путем firewall-а и rutera. Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључење на интернет, односно прикључење преко сопственог модема. Корисници ИКТ система којима је одобрено коришћење интернета дужни су да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени - корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши ИТС ЈППЕУ Ресавица. Приликом коришћења интернета корисник ИКТ система коме је одобрено коришћење интернета дужан је избегавати сумњиве WEБ странице, у циљу спречавања инсталирања програма који могу нанети штету ИКТ систему. У случају да корисник примети необично понашање рачунара, ту појаву је дужан да без одлагања пријави надлежном субјекту ИКТ система. Кориснику ИКТ система коме је дозвољено коришћење интернета забрањено је гледање филмова и играње игрица на рачунарима и

претраживање WEБ страница које садрже порнографски и остали недоличан садржај, као и самовољно преузимање истих са интернета.

Недозвољена употреба интернета обухвата и:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друга врста недозвољених софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено одлуком надлежног органа Оператора;
- преузимање података у количини која проузрокује велико оптерећење на мрежи;
- преузимање материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом;

ИТС ЈППЕУ Ресавица као надлежни субјект ИКТ система има право да уколико се утврди неко од недозвољених употреба Интернета ограничи приступ одређеним web страницама као и да укинуте приступ Интернету одређеном запосленом/кориснику у случају доказане злоупотребе истог.

- Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намена коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

Споразуми о поверљивости или неоткривању штите информације ЈППЕУ Ресавица и обавезују потписнике да информације штите, користе и објављују их на одговоран и

ауторизован начин. Размена података који су означени ознаком тајности са другим органима, организацијама или правни лицима се врши у складу са потписаним актом о размени података.

### *23. Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система*

Члан 28.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, ЈППЕУ Ресавица је у обавези да обезбеди безбедност информација у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења. Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у ЈППЕУ Ресавица, биће дефинисан уговором који ће бити склопљен са тим лицима. Директор ИТ сектора је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица. О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система администратор система мора да води документацију. Документација из претходног става мора да садржи описе свих процедура а посебно процедура које се односе на безбедност ИКТ система.

У захтеве за нове информационе системе или за побољшање постојећих информационих система морају бити укључени захтеви који се односе на безбедност информација и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Захтеви за безбедност информација укључују:

- Проверу идентитета корисника;
- Доступност, поверљивост, непорецивост и интегритет података и имовине;
- Надгледање пословних процеса;

- Омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке кориснике.

Спецификација захтева мора узети у обзир аутоматску контролу која ће бити уведена у информациони систем и потребу да такође постоји и ручна контрола, која мора бити примењена при вредновању пакета софтвера, развијених или купљених, за пословне апликације. Системски захтеви за информациону безбедност и процеси за увођење безбедности се интегришу у фази дизајнирања информационих система. Формално тестирање и процес имплементације ће се примењивати за све купљене производе. У уговору са набављачем за купљене производе дефинишу се захтеви безбедности. У случају да безбедносна функционалност предложеног производа не задовољава одређен захтев, ризик и повезане контроле ће бити преиспитане пре куповине производа.

*24. Заштита података који се користе за потребе тестирања ИКТ система односно делова система*

Члан 29.

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера наведених у овом члану.

За потребе испитивања и тестирања ИКТ система, односно делова система, ЈППЕУ Ресавица избегава коришћење оперативних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачног добављача, купца, запосленог или др. Уколико се за сврху испитивања користе лични подаци или неке друге поверљиве информације, онда се сви осетљиви

подаци и информације пре коришћења штите анонимизацијом личних података, уклањањем садржаја или изменом текста садржаја у предметном делу.

*25. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга*

Члан 30.

Уговори који се закључују са трећим лицима - пружаоцима услуга који имају приступ информацијама, средствима и опреми за обраду информација ЈППЕУ Ресавица морају да садрже одредбу о заштити и чувању поверљивости информација, података и документације. Пружаоци услуга имају право на приступ ресурсима ИКТ система и информацијама које су потребне за пружање уговорене услуге уз поштовање безбедности ИКТ система и интегритета ЈППЕУ Ресавица. Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ. Директор ИТ сектора је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

*26. Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга*

Члан 31.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, ЈППЕУ Ресавица успоставља мере надзора и заштите за време пружања услуга и након извршеног посла. Запослени у ИТС-у редовно прате, анализирају, преиспитују и проверавају извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

- Неопходно је да се поштују сви услови из споразума у вези са безбедношћу информација, као и да се спрече сви инциденти и проблеми нарушавања безбедности, те омогући управљање на одговарајући начин;

- Врши се оцена квалитета извршења и саобразности уговорене услуге;
- Пружалац услуге има уговорну обавезу да организује и припреми периодичне састанаке који ће обезбедити редовно извештавање ЈППЕУ Ресавица и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;
- Директор ИТС-а одржава потпуну контролу над спровођењем услуга и осигурава увид у све осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа страна приступа, процесира или којима управља;
- Преиспитује трагове провере и записа о догађајима у вези са безбедношћу код пружаоцем услуга, оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене; утврдити поступак извештавања, праћења и поступања у складу са захтевима ЈППЕУ Ресавица у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета пружаоца услуга.

Приликом надзора над извршењем квалитета и саобразности уговорене услуге проверава се да ли пружалац услуге задовољава све критеријуме који су били од пресудног значаја приликом избора, укључујући обим и квалитет услуге, као и да се у току поступка извршења услуге може утицати на побољшање квалитета услуге или начина и обима извршења, у складу са утврђеним стварним потребама ЈППЕУ Ресавица.

*27. Превенција и реаговање на безбедносне инциденте, што подразумева адекватну* размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама

Члан 32.

Сви запослени су у обавези да извештавају о уоченим и утврђеним слабостима ИКТ система ИТС-у ЈППЕУ Ресавица, у што краћем року, како би се инциденти нарушавања безбедности информација спречили и спречио настанак штете. Догађаји у вези са безбедношћу информација се оцењују и у складу са тим се доноси одлука да ли је

потребно да се класификују као инциденти нарушавања безбедности информација. . Запослени у ИТС-у  благовремено прикупљају информације о безбедносним ризицима, техничким рањивостима информационих система који се користе, вреднују изложеност тим ризицима и рањивостима и предузимају одговарајуће мере, узимајући у обзир степен припадајућих ризика. Запослени у ИТС-у  врше анализу ИКТ система и утврђују степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузимају одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

Уколико се идентификују ризици и рањивости које могу да угрозе безбедност ИКТ система, запослени у ИТС-у су дужни да одмах изврше подешавања, односно инсталирају алат (софтвер) који ће отклонити уочене ризике и слабости.

Смернице за откривање безбедносно-техничких слабости и ризика су:

- када је могућа техничка рањивост идентификована, тада се идентификују припадајући ризици и акције које треба предузети; такве акције могу да обухвате исправке рањивих система и/или примену других контрола;
- најпре се узимају у разматрање системи са високим ризиком;
- у зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, предузете активност се спроводе у складу са контролама које су везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности;
- исправке се морају прво испробати и вредновати пре него што се трајно угради, како би се осигурало да ће оне бити ефективне и да неће довести до споредних утицаја који се не могу толерисати;

• ако исправка није на располагању, онда треба размотрити друге контроле, као што су деактивирање услуга, прилагођавање или додавање контрола приступа или појачано надгледање како би се открили или спречили постојећи напади и утицало на повећање свести о ризицима и опасностима;

Сви запослени морају одмах известити запослене у ИТС-у  о догађајима у вези са угроженом безбедношћу ИКТ система, података и информација. Могуће методе комуникације су: електоронска  пошта, веб сајтови (интерни, екстерни, портали), телефонска комуникација, говорна порука, писмено извештавање, директан контакт. У случају погрешног или отежаног функционисања компоненти ИКТ система, корисник извештава на исти начин као и у случају догађаја у вези са безбедношћу ИКТ система. ,

Процедура за извештавање:

- Запослени који сматра да је дошло до неисправности или безбедносне угрожености ИКТ система, напада или злоупотребе података мора одмах пријавити проблем лични, телефоном или уз опис истог послати поруку електронском поштом запосленом у ИТС-у;
- Када је индетификован инцидент запослени је дужан да одмах обавести ИТС, и предузме мере у циљу заштите ресурса ИКТ система;
- Запослени у ИТС-у и овлашћени администратор врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури.
- ЈППЕУ Ресавица дефинише, идентификује и чува информације које могу да служе као доказ у случају покретања казнених мера унутар организације;
- Запослени у ИТС-у воде евиденцију о свим инцидентима, као и пријавама инцидената, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Прикупљено знање из детектовања, анализе и решавања инцидената који су нарушили безбедност информација, ЈППЕУ Ресавица користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената. Сви запослени су обавезни да се придржавају и спроводе одедбе Акта о безбедности и да свакодневно и доследно спроводе мере и воде бригу у циљу заштите система ИКТ система и безбедности информација.

*28. Мере које обезбеђују континуитет обављања посла у ванредним околностима*

Члан 33.

У случају ванредних околности, које могу да доведу до измештања ИКТ система из зграде управе, надлежни субјект ИКТ система је дужан да у најкраћем року пренесе делове ИКТ система неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама. Спецификацију делова ИКТ система који су неопходни за функционисање у ванредним ситуацијама израђује надлежни субјект ИКТ система, у три примерка, од којих се један налази код њега, други код запосленог надлежног за послове одбране и ванредне ситуације, а трећи примерак код непосредног руководиоца.  Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди непосредни руководилац. Складиштење делова ИКТ система који нису неопходни врши се на начин да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води. У случају немогућности функционисања ИКТ система због вандредних околности, запослени у ИТС-у су дужни да након поновног успостављања функционисања унесу све податке о процедурама које су предузимали у току отказа система.

## III. Прелазне и завршне одредбе

*Посебна обавеза ЈППЕУ Ресавица*

Члан 34.

Обавеза ЈППЕУ Ресавица је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему ЈППЕУ Ресавица о чему сачињава извештај.

*Садржај извештаја о провери ИКТ система*

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава;

2) време провере;

3) подаци о лицима која су вршила проверу;

4) извештај о спроведеним радњама провере;

5) закључке по питању усклађености Правилника о безбедности ИКТ система са прописаним условима;

6) закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;

7) закључке по питању евентуалних безбедносних слабости на нивоу техничких

карактеристика компоненти ИКТ система;

8) оцена укупног нивоа информационе безбедности;

9) предлог евентуалних корективних мера;

10) потпис одговорног лица које је спровело проверу ИКТ система.

*Ступање на снагу Акта о безбедности*

Члан 35.

Овај Акт ступа на снагу наредног дана од дана објављивања на огласној табли и интернет страници ЈППЕУ Ресавица.

У Ресавици, дана 21. 9. 2020.

в.д. Директор ЈППЕУ Ресавица

Марко Вуковић дипл. инж. рударства