Акционарско друштво за железнички превоз путника „Србија Воз“ Београд
**СЕКТОР ЗА ИНФОРМАЦИОНО КОМУНИКАЦИОНЕ ТЕХНОЛОГИЈЕ**
11000 Београд, Немањина 6, тел: +381 11 361 8442

Број:20/2019-163
Датум: 27.02.2019.год.

# Акт о безбедности ИКТ система

## Информације о документу

| Основне информације о документу | |
|---|---|
| Назив документа: | Акт о безбедности ИКТ система |
| Број документа: | 20/2019-163 |
| Датум: | 27.02.2019 |
| Дистрибутивна листа: | запослени у „Србија воз“ а.д. |

# Садржај

# 1. Циљ

Овај Акт, у складу са Законом, одређује мере заштите, принципе, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја. Према Закону о информационој безбедности и Уредби о утврђивању листе послова у областима у којима се обављају делатности од општег интереса у којима се користе ИКТ системи од посебног значаја, а у Члану 2, тачка 4 ове уредбе, утврђено је да су делатности у области железничког, поштанског и ваздушног саобраћаја од посебног значаја, те самим тим и ИКТ систем предузећа Србија Воз а.д подлеже примени овог Закона.

# 2. Дефиниције

**Информационо-комуникациони систем (ИКТ систем)** је технолошко-организациона целина која обухвата:

(1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
(2) 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;
(3) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из (1) и (2) а у сврху њиховог рада, употребе, заштите или одржавања;
(4) организациону структуру путем које се управља ИКТ системом;

**Оператор ИКТ система** је правно лице, орган јавне власти или организациона јединица органа јавне власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

**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;

**Тајност** је својство које значи да податак није доступан неовлашћеним лицима;

**Интегритет** значи очуваност изворног садржаја и комплетности податка;

**Расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

**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;

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

**Ризик** значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

**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;

**Инцидент** је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

**Мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

**Тајни податак** је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

**ИКТ систем за рад са тајним подацима** је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

**Орган јавне власти** је државни орган, орган аутономне покрајине, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, правно лице које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе, као и правно лице које се претежно, односно у целини финансира из буџета;

**Служба безбедности** је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије;

**Самостални оператори ИКТ система** су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове и службе безбедности;

**Компромитујуће електромагнетно зрачење** (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

**Криптобезбедност** је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

**Криптозаштита** је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

**Криптографски** производ је софтвер или уређај путем кога се врши криптозаштита;

Криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

**Безбедносна зона** је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

**Информациона добра** обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и слично.

**Тим за спровођење мера Акта о безбедности ИКТ система предузећа** (даље у тексту: ***Тим за безбедност ИКТ система***) је субјект формиран Одлуком надлежног руководства предузећа одговоран за спровођење и праћење примене мера Акта о безбедности ИКТ система.

# 3. Основни принципи

Управљање информационом безбедношћу ИКТ система предузећа Србија Воз а.д. се заснива на следећим принципима и начелима:

- **Начело управљања ризиком** подразумева да се избор и примена мера заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући и све врсте ванредних околности.
- **Начело свеобухватне заштите** подразумева да се све мере примењују на свим организационим, физичко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система.
- **Начело стручности и добре праксе** подразумева да се мере примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности.
- **Начело свести и оспособљености** подразумева да сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесна ризика и поседују одговарајућа знања и вештине.

Сва ова описана начела и принципи су уткани у сва интерна Акта Србија Воз а.д. који се тичу информационе безбедности, али и у осталим актима где је то било потребно како би се примениле слојевите административне и техничке контроле у свеобухватном смислу, тј. на нивоу целог предузећа.

## 3.1. Измене Акта о безбедности ИКТ система

Акт о безбедности ИКТ система мора да буде усклађен са променама у окружењу и у самом ИКТ систему.
Промене у окружењу и у самом ИКТ систему су оне промене које могу довести до повећане изложености ИКТ система безбедносним ризицима, услед наступања:

- техничко-технолошких,
- кадровских,
- организационих промена

У случају горе поменутих промена, уколико је то потребно, врши се измена Акта о безбедности, односно прилагођавање и унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и

преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

## 3.2. Провера ИКТ система

Србија Воз а.д. се обавезује да врши проверу ИКТ система, односно проверу усклађености примењених мера заштите са Актом о безбедности. Провера може да се врши самостално или уз ангажовање спољних експерата. Провером се утврђује испуњеност услова за мере заштите прописаних законом и Уредбом о мерама заштите. Провером се оцењује адекватност нивоа информационе безбедности путем провере мера заштите, процедура и одговорности утврђених овим Актом.
Провером се утврђује угроженост или нарушавање информационе безбедности која настаје коришћењем неодговарајућих поступака и техничких средстава. Србија Воз а.д. се обавезује да проверу врши најмање једном годишње и да о томе сачини извештај.

Извештај о провери ИКТ система мора да садржи следеће:

- назив оператора ИКТ система који се проверава
- време провере
- начин провере – самостално или уз ангажовање спољних експерата
- испуњеност услова прописаних законом и подзаконским актима
    - донесен Акта о безбедности
    - предвиђене одговарајуће мере заштите на бази адекватне анализе ризика
    - дефинисане процедуре за спровођење мера заштите
    - дефинисана овлашћења и одговорности
- оцена примене предвиђених мера заштите
- оцена укупног нивоа информационе безбедности
- предлагање мера за унапређење безбедности ИКТ система и измену Акта о безбедности
- потпис одговорног лица које је спровело проверу ИКТ система, или потпис, односно печат спољног експерта.

## 3.3. Мере заштите ИКТ система

Србија Воз а.д. је одговорна за безбедност ИКТ система и предузимање мера за заштиту. Мерама заштите се обезбеђује превенција од настанка инцидената, односно превенција и умањене штете од инцидената који угрожавају обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Србија Воз а.д. спроводи мере заштите дефинисане Законом о информационој безбедности, одржава спровођење и врши контролу ефективности тих контрола.

## 3.4. Поверавање активности у вези са ИКТ системом трећим лицима

Србија Воз а.д. може поверити активности у вези са ИКТ системом трећим лицима, у ком случају је обавезна да уреди однос са тим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом.

Повераваним активностима сматрају се све активности које укључују обраду, чување, односно могућност приступа подацима којима располаже Србија Воз а.д. , а односе се на пословање самог предузећа.
Под трећим лицем сматра се и привредни субјекат који је имовинским и управљачким односима (лица са учешћем, чланице групе друштава којој тај привредни субјект припада и др.) повезан са предузећем Србија Воз а.д.
Поверавање активности врши се на основу уговора закљученог између предузећа Србија Воз а.д. и лица коме се те активности поверавају или посебним прописом.

Поверавање активности мора бити и у складу са другим регулаторним обавезама које покривају делатност Србија Воз а.д..

## 3.5. Обавештавање надлежног органа о инцидентима

Србија Воз а.д. је у обавези да обавести надлежни орган о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности. Надлежни орган за институције од посебног значаја национални ЦЕРТ.

Поступак достављања података, листу, врсте и значај инцидента и поступак обавештавања је дефинисан Законом и интерна акта Србија Воз а.д. су усаглашена са свим одредбама из Закона и свих релевантних уредби.

Ако је инцидент од интереса за јавност, надлежни орган коме се упућују обавештења о инцидентима, може наложити његово објављивање. Такође, уколико је инцидент везан за извршење кривичних дела која се гоне по службеној дужности, надлежни орган обавештава јавно тужилаштво, односно министарство надлежно за унутрашње послове.

Ако је инцидент повезан са нарушавањем права на заштиту података о личности, надлежни орган о томе обавештава и Повереника за информације од јавног значаја и заштиту података о личности.

## 3.6. Превенција и заштита од безбедносних ризика у ИКТ системима у Републици Србији

Закон предвиђа формирање Националног центра за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ) и својим садржајем ближе уређује послове координације, превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији.

У интересу предузећа Србија Воз а.д. је учествовање у ЦЕРТ-у и овим Актом Србија Воз а.д. потврђује спремност за партиципирање у централизованом ЦЕРТ систему на националном нивоу у било којој форми предвиђеној Законом. Пре уписивања у ЦЕРТ регистар Србија Воз а.д. је сагласна да усагласи све захтеве предвиђене Законом.

# 4. Примењене мере заштите

У складу са Законом и релевантним Уредбама, као и са тачком 3.3 овог Акта, Србија Воз а.д. врши примену свеобухватних мера за свих 28 области, а релевантни интерни акти којим су ове области ближе дефинисане се налазе у прегледу примењених мера који су презентовани у Прилогу 1 овог Акта.

# 5. Одговорности и овлашћења

Обавезу и одговорност за поступање у складу са процедуром имају сви запослени у предузећу Србија Воз а.д. који учествују у процесу израде, одобравања, измене и замене документа, као и запослени који тај документ примењују.

Власник документа одговоран за сачињени текст и тачност података у документу, као и за имплементацију и решавање евентуалних спорних ситуација је Тим за спровођење мера Акта о безбедности ИКТ система предузећа.

Све одговорне особе у поступку израде, провере и одобравања примене овог документа, као и сви корисници, дужни су да се, сходно Уговору о раду, придржавају обавезе чувања поверљивих информација везаних за пословање предузећа Србија Воз а.д.

# Прилог 1: Преглед докумената мера заштите „Србија Воз“а.д. у области информационе безбедности

| РБ | Мере заштите дефинисане у Закону о информационој безбедности | Документа која ближе дефинишу Мере заштите примењене у „Србија Воз“ а.д. |
|---|---|---|
| 1 | Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система | Правилник о унутрашњој организацији (Правилник о систематизацији и Уговори о раду)<br>Управљање инцидентима |
| 2 | Постизање безбедности рада на даљину и употребе мобилних уређаја | Управљање ИТ инфраструктуром<br>Управљање мобилним уређајима |
| 3 | Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност | Правилник о унутрашњој организацији (Правилник о систематизацији и Уговори о раду) |
| 4 | Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система | Правилник о унутрашњој организацији (Правилник о систематизацији и Уговори о раду)<br>Управљање ИТ инфраструктуром<br>Изјава о поверљивости |
| 5 | Идентификовање информационих добара и одређивање одговорности за њихову заштиту | Централни регистар информационих добара<br>Класификација и означавање информација |
| 6 | Класификовање података | Централни регистар информационих добара<br>Класификација и означавање информација |
| 7 | Заштита носача података | Правило Бекапа<br>Управљање ИТ инфраструктуром<br>Класификација и означавање информација |
| 8 | Ограничење приступа подацима и средствима за обраду података | Управљање ИТ инфраструктуром<br>Класификација и означавање информација<br>Политика чистог стола и екрана |
| 9 | Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа | Управљање ИТ инфраструктуром<br>Политика чистог стола и екрана |
| 10 | Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију | Управљање ИТ инфраструктуром<br>Правилник о унутрашњој организацији |
| 11 | Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података | Управљање ИТ инфраструктуром<br>Правило Бекапа<br>Правило комуникације са трећим лицима |
| 12 | Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему | Правилник о физичко-техничком обезбеђењу имовине и лица<br>Управљање ИТ инфраструктуром |
| 13 | Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем | Управљање ИТ инфраструктуром<br>Класификација и означавање информација<br>Управљање мобилним уређајима |

| РБ | Мере заштите дефинисане у Закону о информационој безбедности | Документа која ближе дефинишу Мере заштите примењене у „Србија Воз“ а.д. |
|---|---|---|
| 14 | Обезбеђивање исправног и безбедног функционисања средстава за обраду података | Управљање ИТ инфраструктуром<br>Правило Бекапа<br>Правилник о физичко-техничком обезбеђењу имовине и лица |
| 15 | Заштита података и средства за обраду података од злонамерног софтвера | Управљање ИТ инфраструктуром<br>Правило управљања закрпама |
| 16 | Заштита од губитка података | Управљање ИТ инфраструктуром<br>План континуитета рада информационог система<br>Правило Бекапа |
| 17 | Чување података о догађајима који могу бити од значаја за безбедност ИКТ система | Процедура за надгледање информационог система и апликација |
| 18 | Обезбеђивање интегритета софтвера и оперативних система | Процедура за надгледање информационог система и апликација<br>Управљање изменама у ИТ систему<br>Правило управљања закрпама<br>Правило Бекапа<br>Управљање пројектима |
| 19 | Заштита од злоупотребе безбедносних слабости ИКТ система | Управљање изменама<br>Правило управљања закрпама<br>Управљање ИТ инфраструктуром |
| 20 | Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система | Управљање изменама |
| 21 | Заштита података у комуникационим мрежама укључујући уређаје и водове | Управљање ИТ инфраструктуром<br>Класификација и означавање информација |
| 22 | Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система | Класификација и означавање информација<br>Правило комуникације са трећим лицима<br>Уговор о поверљивости података<br>Уговор са добављачем – члан о поверљивости |
| 23 | Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система | Управљање ИТ инфраструктуром |
| 24 | Заштита података који се користе за потребе тестирања ИКТ система односно делова система | Управљање ИТ инфраструктуром |
| 25 | Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга | Класификација и означавање информација<br>Процедура за надгледање информационог система и апликација<br>Уговор са добављачем – члан о поверљивости<br>Правило комуникације са трећим лицима |
| 26 | Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга | Процедура за надгледање информационог система и апликација<br>Уговор са добављачем – члан о поверљивости<br>Уговор о поверљивости |

| РБ | Мере заштите дефинисане у Закону о информационој безбедности | Документа која ближе дефинишу Мере заштите примењене у „Србија Воз“ а.д. |
|---|---|---|
| 27 | Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама | Управљање инцидентима |
| 28 | Мере које обезбеђују континуитет обављања посла у ванредним околностима | План континуитета пословања и оправка система<br>Правило Бекапа |

**ДИРЕКТОР СЕКТОРА ЗА**
**ИНФОРМАЦИОНО-КОМУНИКАЦИОНЕ ТЕХНОЛОГИЈЕ**

**Драган Ранковић**