**Република Србија**
**ОСНОВНО ЈАВНО ТУЖИЛАШТВО**
**А.бр.161/20**
**01.11.2020.године**
**Ј а г о д и н а**

# АКТ О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

## ОСНОВНЕ ОДРЕДБЕ

### Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система, у складу са Законом оинформационој безбедности („Службени гласник РС”, број 6/16, у даљем тексту:Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система (у даљемтексту: ИКТ систем).

### Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

1) одређивање начина и процедура за постизање и одржавање адекватног ниво абезбедности система;
2) спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
3) подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4) прописивање овлашћења и одговорности запослених у вези са безбедношћу иресурсима ИКТ система;
5) свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

**Обавеза примене одредби Акта о безбедности**

Члан 3.

Мере заштите ИКТ система које су ближе уређене Актом о безбедности служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за све запослене. Запослени морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

**Одговорност запослених**

Члан 4.

Запослени су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

**Предмет заштите**

Члан 5.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

## I. МЕРЕ ЗАШТИТЕ

**Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система**

Члан 6.

Организациона структура представља скуп задатака и овлашћења којим се уређује начин на који запослени обављају своје активности и користе расположиве ресурсе запостизање циљева организације.

Члан 7.

Оператор ИКТ система се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају.

**Заштита од ризика који настају при променама послова или престанка радногангажовања запослених лица**

Члан 8.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања.

**Идентификовање информационих добара и одређивање одговорности за њиховузаштиту**

Члан 9.

Информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

**Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности**

Члан 10.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем.

**Заштита носача података**

Члан 11.

Оператор ИКТ система обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података.

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

Члан 12.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности података.

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

Члан 13.

Оператор ИКТ система управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

**Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију**

Члан 14.

Аутентификације корисника којима је одобрен приступ систему врши се путем јединственог корисничког имена и шифре.

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

Члан 15.

У циљу заштите података Оператор ИКТ система развија и имплементира политику коришћења криптографских контрола, и успоставља механизме и систем зауправљање кључевима.

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

Члан 16.

Оператор ИКТ система је дужан да предузме мере ради спречавања неовлашћеног физичког приступа објекту, простору, просторијама, зони, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација и опреме за обраду информација.

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

Члан 17.

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

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

Члан 18.

Усвајање и примена радних процедура.

Оператор ИКТ система 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, укључујући ограничења у коришћењу системских помоћних функција;

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.

**Заштита података и средстава за обраду података од злонамерног софтвера**

Члан 19.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен или неумрежен рачунар. Заштита од злонамерног софтвера се заснива на софтверу за откривање злонамерног софтвера и отклањање штете, на познавању безбедности информација, као и на одговарајућим контролама приступа систему и управљања захтеваним и потребним променама.

**Заштита од губитка података**

Члан 20.

Оператор ИКТ система врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног системау случају наступања последица изазваних ванредним околностима.

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

Члан 21.

У ИКТ систему формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

**Обезбеђивање интегритета софтвера и оперативних система**

Члан 22.

Оператор ИКТ система спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система у складу са смерницама за контролу промена и инсталацију софтвер.

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

Члан 23.

Оператор ИКТ система 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.

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

Члан 24.

Приликом спровођења ревизије ИКТ система, Оператор ИКТ система обезбеђује даревизија има што мањи утицај на функционисање система.

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

Члан 25.

Заштита података који се преносе комуникационим средствима обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

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

Члан 26.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, Оператор ИКТ система 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.

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

Члан 27.

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.

**Заштита средстава оператора ИКТ система која су доступна пружаоцимауслуга**

Члан 28.

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

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

Члан 29.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, Оператор ИКТ система успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

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

Члан 30.

Посебним процедурама се уређује начин одговора на инциденте нарушавања безбедности информација и одређује особа за контакт у случајевима нарушавања безбедности, као и контакте са овлашћеним телима.

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

Члан 31.

Оператор ИКТ система примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

**ОСНОВНИ ЈАВНИ ТУЖИЛАЦ**

**Александар Цветковић**