Република Србија
ВИШЕ ЈАВНО ТУЖИЛАШТВО У СОМБОРУ
С О М Б О Р
Посл. број: А 54/2022
Датум: 23.03.2022.

На основу члана 34 Закона о јавном тужилаштву ("Службени гласник РС" бр.116/2008..106/2015, 63/2016 – одлука УС), члана 2 Правилника о управи у јавним тужилаштвима („Службени гласник РС", бр. 57/2019) и одредаба Закона о информационој безбедности (Службени гласник РС", број 6/2016) Виши јавни тужилац у Сомбору Зоран Дивјак доноси

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 о информационој 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 увези са безбедношћу и ресурсима информационо-комуникационог система (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

1) одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности 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;

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 радног ангажовања 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 њихову заштиту

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.

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 система у случају наступања последица изазваних ванредним околностима.

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 пружаоцима услуга

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.