Република Србија
ОСНОВНО ЈАВНО
ТУЖИЛАШТВО У АРАНЂЕЛОВЦУ
А бр. 407/20
18.11.2020. године
А р а н ђ е л о в а ц
ЗН/НМ

МИНИСТАРСТВО ТРГОВИНЕ, ТУРИЗМА И ТЕЛЕКОМУНИКАЦИЈА
- **Сектор за информационо друштво и информациону безбедност –**

БЕОГРАД
Ул. Немањина бр. 22-26

У прилогу дописа шаљемо Вам формиран Правилник о безбедности информационо комуникационог система Основног јавног тужилаштва у Аранђеловцу.

ОСНОВНИ ЈАВНИ ТУЖИЛАЦ
Зоран Ивановић

РЕПУБЛИКА СРБИЈА Основно јавно тужилаштво у Аранђеловцу АРАНЂЕЛОВАЦ

Република Србија
ОСНОВНО ЈАВНО
ТУЖИЛАШТВО У АРАНЂЕЛОВЦУ
А бр. 407/20
03.11.2020. године
А р а н ђ е л о в а ц

На основу члана 8. Закона о информационој безбедности („Службени гласник РС" број 6/2016 и 94/2017), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо комуникационих система од посебног значаја, начину провере информационо комуникационих система од посебног значаја и садржају извештаја о провери информационог комуникационог система од посебног значаја („Службени гласник РС" број 94/2016) и члана 39. Закона о агенцији за борбу против корупције („Службени гласник РС“, број 97/2008, 53/2010, 66/2011, 67/2013, 8/2015, Основни јавни тужилац у Аранђеловцу дана 03.11.2020. године доноси;

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО КОМУНИКАЦИОНОГ СИСТЕМА ОСНОВНОГ ЈАВНОГ ТУЖИЛАШТВА У АРАНЂЕЛОВЦУ

УВОДНЕ ОДРЕДБЕ

Члан 1.

Овим Правилником уређују се мере заштите од безбедносних ризика у информационо комуникационом систему Основног јавног тужилаштва у Аранђеловцу, начин и процедуре постизања и одржавања адекватног нивоа безбедности, и овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система тужилаштва.

Члан 2.

Мере прописане овим Правилником односе се на сва запослена лица, тј. на Основног јавног тужиоца, заменике Основног јавног тужиоца и целокупно тужилачко особље.

Члан 3.

Поједини термини у смислу овог Правилника имају следеће значење:

1) Информационо комуникациони систем (икт систем) је технолошко организациона целина која обухвата све уређаје за електронску обраду података (хардверске и софтверске компоненте, мрежу и мрежне ресурсе, сервер и осталу комуникациону опрему);
2) Оператор ИКТ система је Основно јавно тужилаштво у Аранђеловцу као орган јавне власти, тј. државни орган:
3) Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, да буду доступни, употребљиви на захтев овлашћених лица онда када су им потребни, да се очува изворни садржај и комплетност података, да се предупреде ризици и да се адекватно врши управљање ризицима;
4) Ризик подразумева могућност нарушавања информационе безбедности;
5) Управљање ризиком подразумева скуп мера (планирање, организовање и усмеравање активности) у циљу обезбеђења да ризици остану у прописаним и прихватљивим оквирима;
6) Инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
7) Мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима;
8) Тајност је својство које значи да податак није доступан неовлашћеним лицима;
9) Тајни податак је податак који је у складу са Прописима о тајности података одређен и означен одређеним степеном тајности
10) Backup је резервна копија података;
1) UPS (UNINTERUPTABLE POWER SUPPLY) је уређај за непрекидно напајање електричном енергијом;
12) USB или флеш меморија је спољашњи медијум за складиштење података:
13) CD-ROM (COMPACT DISK - READ ONLY MEMORY) и DVD су медијуми за снимање и складиштење података:
14) Информациона добра обухватају пословне информације, тј. средства путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података, укључујући све електронске записе, рачунарску опрему, сервер, мрежну опрему, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, интерне акте који се односе на ИКТ систем и слично.

МЕРЕ ЗАШТИТЕ

Члан 4.

Мерама зашите се обезбеђује превенција од настанка инцидената, односно

превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности.

Мере заштите ИКТ система обухватају следеће послове:
1) Успостављање организационе структуре са утврђеним пословима и одговорностима запослених, који су оспособљени за посао који раде и разумеју своју одговорност;
2) Ограничење приступа подацима и средствима за обраду података (рачунарима);
3) Онемогућавање, односно спречавање неовлашћене или ненамерне измене, губитка, оштећења и злоупотребе података и средстава за обраду података;
4) Заштита података и средстава за обраду података од злонамерног софтвера;
5) Обезбеђивање исправног и безбедног функционисања средстава за обраду података;
6) Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код Оператора ИКТ система;
7) Физичка заштита објеката, простора, просторија, односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;
8) Превенција и реаговање на безбедносне инциденте, пријављивање недостатака и предлагање одговарајућих мера у циљу побољшања информационе безбедности.

АДМИНИСТРАТОР ИКТ СИСТЕМА

Члан 5.

ИКТ системом управља и руководи запослени који поседује администраторски налог, у складу са описом послова из важећег акта о систематизацији радних места. Администраторски налог је јединствени налог којим је омогућен приступ и администрацији свих ресурса ИКТ система, као и отварање нових и измена постојећих налога. Запослено лице које 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. Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог, односно надлежног руководиоца.

Запослени који управља ИКТ системом (администратор) дужан је да сваког новог корисника упозна са одговорностима и правилима коришћења ИКТ ресурса Основног јавног тужилаштва у Аранђеловцу и да води евиденцију о изјавама новозапослених корисника да су упознати са правилима коришћења ИКТ ресурса. Евиденцију о информационим добрима Основног јавног тужилаштва у Аранђеловцу води администратор ИКТ система у папирној или електронској форми.

НАЛОЗИ КОРИСНИКА

Члан 6.

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира на тај начин што се прво уписује име, па презиме запосленог, који су одвојени тачком и куцају се латиничним писмом без употребе слова Ђ, Ж, Љ, Њ, Т, Ч, Ц, Ш.

Уместо ћириличних слова наведених у претходном ставу користе се латиничне ознаке за иста, и то: DJ; Ж- Z, D-LJ, H-NJ, -S, Ч-S, J-DZ, II-S.

Лозинка корисника мора да садржи минимум осам карактера комбинованих од малих и великих слова, цифара и специјалних знакова. Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке запосленог.

Ако корисник посумња да је друго лице открило негову лозинку дужан је да исту одмах измени.

Корисник је дужан да мења лозинку на свака два месеца.

Иста лозинка се не сме понављати у временском периоду од шест месеци.

Члан 7.

Корисник може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору за подешавање корисничког профила и радне странице. Кориснички налог додељује администратор у сарадњи са непосредним руководиоцем. За послове извршене под одређеним корисничким именом и лозинком одговоран је корисник ИКТ система коме је корисничко име, тј. налог додељен. Неовлашћено уступање корисничког налога другом лицу подлеже дисциплинској одговорности.

НАДЗОР И КОНТРОЛА ОД СТРАНЕ АДМИНИСТРАТОРА

Члан 8.

Администратор ИКТ система у обавези је да континуирано надзире и проверава функционисање средстава за обраду података, да управља ризицима који могу утицати на безбедност ИКТ система, као и да планира и предлаже руководиоцу одговарајуће мере. Администратор ИКТ система је дужан да проверава да ли се у оперативном раду адекватно примењују предвиђене мере затите и процедуре у складу са утврђеним овлашћењима и одговорностима, да врши проверу безбедносних слабости на нивоу техничких карактерстика компоненти ИКТ система, архитектуре решења, техничке конфигурације, да о извршеној провери сачињава извештај и доставља га руководиоцу. Извештај треба да садржи време провере, спроведене радње, закључке по питању адекватне примене предвиђених мера заштите, закључке по питању евентуалних

безбедносних слабости, оцену стања у погледу информационе безбедности, предлог евентуалних корективних мера, и потпис лица које је спровело проверу ИКТ система.

ПРЕСТАНАК РАДНОГ ОДНОСА ЗАПОСЛЕНОГ И ПРОМЕНА РАДНОГ МЕСТА И ОВЛАШЋЕЊА

Члан 9.

У случају промене радног места, односно овлашћења корисника, администратор ИКТ система ће извршити промену права у коришћењу ИКТ система, у складу са описом радних задатака и захтевом руководиоца корисника. У случају престанка радног ангажовања корисника, његов кориснички налог се гаси тј. укида. О престанку радног односа или радног ангажовања, као и промени радног места корисника, руководилац је дужан да обавести администратора ИКТ система ради укидања, односно измене приступних налога тог корисника. Корисник је након престанка правног основа по коме је приступао ресурсима ИКТ система Основног јавног тужилаштва у Аранђеловцу, у обавези да не открива податке који су од значаја за информациону безбедност ИКТ система.

ПРЕНОСИВИ МЕДИЈИ И АНТИВИРУСНА ЗАШТИТА

Члан 10.

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, имејлом, зараженим преносним медијима (USB меморијом, CD-от, итд), инсталацијом нелиценцираног софтвера и слично. За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски у тачно одређено време врши допуна антивирусних дефиниција. Забрањено је заустављање и искључивање антивирусног софтвера. Преносиви медији (USB меморија, CD) пре коришћења морају бити проверени на присуство вируса од стране администратора ИКТ система. У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави администратору ИКТ система.

ПОСТУПАЊЕ СА ОПРЕМОМ ИКТ СИСТЕМА

Члан 11.

Право приступа простору у коме се налазе сервери, мрежна и комуникациона опрема има само администратор ИКТ система. У простору је неопходно успоставити и одржавати одговарајућу температуру, у складу са важећим стандардима (климатизован простор).

Прозори и врата на просторији из става 1. овог члана морају увек бити затворени. Сервер и мрежна опрема (Switch, Modem, Router, Firewal) морају стално

бити прикључени на уређаје за непрекидно напајање-UPS. У случају нестанка електричне енергије у периоду дужем од капацитета UPS-а, администратор ИКТ система је дужан да искључи опрему у складу са процедурама произвођача опреме. Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходно стабилну верзију. Инсталирање новог софтвера, као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запосленог-корисника.

Члан 12.

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) се мора налазити у закључаном Rack орману. Администратор ИКТ система врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Члан 13.

У случају изношења опреме ИКТ система ради сервисирања, неопходно је писано одобрење руководиоца. Администратор ИКТ система одређује све детаље везане за изношење опреме и сачињава записник у коме се наводи назив и тип опреме, серијски број, назив сервисера. У случају крајње нужде, у циљу спашавања опреме, иста се може изнети без одобрења руководиоца.

РЕЗЕРВНЕ КОПИЈЕ ПОДАТАКА

Члан 14.

Администратор ИКТ система је у обавези да прави резервне копије базе података најмање једном дневно. Базе података обавезно се архивирају и на преносиве медије (CD Rom, DVD, USB или екстерни хард диск). За потребе обнове базе података сваки примерак преносног информатичког медија са копијама-архивама мора бити означен бројем, врстом (дневна, недељна, месечна, годишња), датумом израде копије-архиве, као и именом запосленог који је извршио копирање-архивирање. Дневне, недељне и месечне копије-архиве се чувају у просторији која је физички обезбеђена у складу са мерама заштите од пожара. Месечне копије података се чувају и ван институције - Основног јавног тужилаштва у Аранђеловцу у случају пожара, поплава н слично. Исправност копија-архива проверава администратор ИКТ система.

Члан 15.

Правилник ступа на правну снагу даном објављивања на огласној табли Основног јавног тужилаштва у Аранђеловцу, где ће бити изложен 30 дана, како би се сви запослени упознали са истим. Правилник објавити и на интернет страници Основног јавног тужилаштва у Аранђеловцу.

Обрадио:

Виши тужилачки сарадник
Нена Мајсторовић

ОСНОВНИ ЈАВНИ ТУЖИЛАЦ
У АРАНЂЕЛОВЦУ
Зоран Ивановић