Република Србија
ВИШЕ ЈАВНО
ТУЖИЛАШТВО У БЕОГРАДУ
А.бр 1178/19
01.10.2019.год.
Б е о г р а д
АМ

На основу чл. 34. Закона о јавном тужилаштву ("Сл. гласник РС", бр. 116/08, 104/09, 101/2010,78/2010,- др.закон, 101/2011, 38/2012-одлука УС, 121/2012, 101/2013, 111/2014- одлука УС, 117/2014, 106/2015 и 63/2016- одлука УС), чл. 8 став 1 Закона о информационој безбедности(Службени гласник РС број 6/16), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо – комуникационог система од посебног значаја (Сл гласник РС 94/2016), Јавни тужилац Вишег јавног тужилаштва у Београду, доноси :

ПРАВИЛНИК ОБЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ВИШЕГ ЈАВНОГ ТУЖИЛАШТВА У БЕОГРАДУ

I

ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим Правилником се у складу са законом утврђују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система(у даљем тексту ИКТ систем), као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система Вишег јавног тужилаштва у Београду.

Овај Правилник је обавезујући за све унутрашње организационе јединице Вишег јавног тужилаштва у Београду и за све кориснике информатичких

ресурса, као и за сва трећа лица која користе информатичке ресурсе Вишег јавног тужилаштва у Београду.

Непоштовање овог Правилника повлачи дисциплинску одговорност корисника информатичких ресурса.

За праћење примене овог Правилника надлежан је Јавни тужилац као и управа Вишег јавног тужилаштва у Београду.

II

ПОЈМОВИ

Члан 2.

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 чл 1 и 2 ове тачке, а у сврху његовог рада, употребе, заштите или одржавања;
4. организациону структуру путем које се управља ИКТ системом;

Два основна метода бележења информација су;

1. мануелно
2. електронско (бар кодови, електронски скенери, оптичко препознавање знакова)

Администратор ИКТ система је 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.

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

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

Информациона добра су сви ресурси који садрже пословне информације, односно свих ресурси путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и сл.

III

ЦИЉ ПРАВИЛНИКА

Члан 3.

Циљеви доношења Акта о безбедности су:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2. спречавање и ублажавање последица инцидента 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 вези са бездношћу и ресурсима ИКТ система;
5. свеукупно унапређење информационе безбедности провера усклађености примене мера заштите;

IV

ПРЕДМЕТ, МЕРЕ И СУБЈЕКТИ ЗАШТИТЕ ИКТ СИСТЕМА

Члан 4.

Предмет заштите ИКТ система су:

1. хардверске и софтверске компоненте ИКТ система
2. подаци који се обрађују или чувају на компонентима ИКТ система
3. кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система.

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидента који угрожавају обављање делатности Вишег јавног тужилаштва у Београду, 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.

Мере прописане овим актом се односе на све организационе јединице ИКТ система Вишег јавног тужилаштва у Београду, на све запослене- кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Вишег јавног тужилаштва у Београду.

Члан 6.

За контролу и надзор над обављањем послова запослених- корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система, надлежан је систем администратор Вишег јавног тужилаштва у Београду.

V

ОБАВЕЗА ПРИМЕНЕ ОДРЕДБИ ПРАВИЛНИКА О БЕЗБЕДНОСТИ И ОДГОВОРНОСТ ЗАПОСЛЕНИХ У ВЈТ у

Члан 7.

Запослени у Вишем јавном тужилаштву морају бити упознати са садржином акта о безбедности и дужни су да поступају у складу са одредбама овог акта.

Систем администратор Вишег јавног тужилаштва дужан је да прати примену мера безбедности и контролише да ли су информације/подаци заштићени на начин који је утврђен овим Правилником и интерним процедурама.

Члан 8.

Запослени у Вишем јавном тужилаштву 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.

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

Непоштовање одредби Правилника о безбедности, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

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 предпостављеног руководиоца.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида.

Корисник ИКТ ресурса, након престанка радног ангажовања у тужилаштву, не сме да открива податке који су од значаја за информациону безбедност ИКТ система.

VI

БЕЗБЕДНОСТ РАДА НА ДАЉИНУ И УПОТРЕБА МОБИЛНИХ УРЕЂАЈА

Члан 10.

Запослени–корисници ресурса ИКТ система, могу путем мобилних уређаја, који су подешени од стране систем администратора, да приступају само одређеним деловима ИКТ система. Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ.

Запосленом-кориснику забрањена је самостална инсталација сефтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима.

У случају квара мобилног уређаја, систем администратор је дужан да пре предаје уређаја овлашћеном сервису, уради копију података који се налазе на мобилном уређају, а потом их избрише из уређаја и по повратку из сервиса врати податке у мобилни уређај.

VII

ОГРАНИЧЕЊЕ ПРИСТУПА ПОДАЦИМА И СРЕДСТВИМА ЗА ОБРАДУ ПОДАТАКА

Члан 11.

Приступ ресурсима ИКТ система одређен је врстом налога који запослени 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 може користити 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 који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.

Члан 12.

Запослени у Вишем јавном тужилаштву у Београду је дужан да поштује следећа правила безбедног и примереног коришћења ресурса ИКТ система:

1. да користи информатичке ресурсе искључиво у пословне сврхе
2. да прихвати да су сви подаци који се складиште, преносе или процесуирају у оквиру информатичких ресурса, власништво Вишег јавног тужилаштва у Београду и да могу бити предмет надгледања и прегледања
3. да поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података,
4. да безбедно чува своје лозинке у односу на друга лица;
5. да се пре сваког удаљавања од радне станице, одјави са система, односно закључа радну станицу;
6. да користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење надлежног субјекта ИКТ система;
7. да захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8. да обезбеди сигурност података у скалду са важећим прописима;
9. да не сме да зауставља рад или брише антивирус програм, мења његове подешене опције,нити да неовлашћено инсталира други антивирус програм
10. да не сме да на радној станици складишти садржај који не служи у пословне сврхе
11. да не израђује заштитне копије(backup) података у складу са прописаним процедурама
12. да користи Internet и Internet e- mail сервис Вишег јавног тужилаштва у Београду у складу са прописаним процедурама,
13. да прихвати да се одређене врсте информатичких интервенција обављају у утврђено време
14. да прихвати инсталацију техника и програма у циљу сигурности ИКТ система

15. да не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.
16. да по завршетку посла односно радног дана прописно искључи рачунар.
17. да је строго забрањено изношење преносивих ИКТ уређаја (лаптопова) ван просторија Вишег јавног тужилаштва у Београду без писменог одобрења

VIII

ОДОБРАВАЊЕ ОВЛАШЋЕНОГ ПРИСТУПА И СПРЕЧАВАЊЕ НЕОВЛАШЋЕНОГ ИКТ СИСТЕМУ И УСЛУГАМА КОЈЕ ИКТ СИСТЕМ ПРУЖА

Члан 13.

Право приступа имају само запослени-корисници који имају администаторске или корисничке налоге. Администраторски налог је јединствени налог којим је омогућен приступ и аминистрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога. Администраторски налог може да користи искључиво систем администратор Вишег јавног тужилаштва у Београду.

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 кадровима у сарадњи са секретаром Вишег јавног тужилаштва у Београду, а у складу са потребама обављања пословних задатака од стране запосленог – корисника.

Систем администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог на пословима управљања кадровима, односно секретара тужилаштва.

IX

УТВРЂИВАЊЕ ОДГОВОРНОСТИ КОРИСНИКА ЗА ЗАШТИТУ СОПСТВЕНИХ СРЕДСТАВА ЗА АУТЕНТИФИКАЦИЈУ

Члан 14.

Кориснички налог се састоји од корисничког имена и лозинке.

Корисничко име се креира латиничним писмом по матрици (име презиме као једна реч раздвојено тачком и без употребе слова ђ,ж,љ,њ,ћ,ч,џ,ш).

Лозинка мора да садржи минимум 7 карактера и не сме да садржи датум рођења, број телефона и друге препознатљиве податке.

Неовлашћено уступање корисничког налога као и медија са електронским сертификатом другом лицу, подлеже дисциплинској одговорности.

X

ФИЗИЧКА ЗАШТИТА ОБЈЕКТА, ПРОСТОРА, ПРОСТОРИЈА –ЗОНЕ У КОЈОЈ СЕ НАЛАЗЕ СРЕДСТА И ДОКУМЕНТИ ИКТ СИСТЕМА

Члан 15.

Простор у коме се налазе рачунари за вођење база података и централни рачунар(сервер), мрежна или комуникациона опрема ИКТ система, организује се као административна зона.

Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видиљиво означеном простору, који је обезбеђен механичком бравом.

Члан 16.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система и особама запосленим у ИКТ служби.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу јавног тужиоца.

Строго је забрањен приступ незапосленим лицима административној зони.

Просторија из става 1. овог члана мора бити видљиво обележена и у њој се мора налазити противпожарна опрема(апарат), која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима.

У случају изношења опреме из просторије из става 1 овог члана ради селидбе, или сервисирања, неопходно је одобрење Јавног тужиоца који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења Јавног тужиоца, потребно је сачинити записник у коме се наводи назив и тип опреме, сријски 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 Вишег јавног тужилаштва у Београду.

Приступ административној зони могу имати и лица која пружају услуге одржавања хигијене Вишег јавног тужилаштва у Београду.

XI

ЗАШТИТА НОСАЧА ПОДАТАКА

Члан 17.

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 Јавног тужиоца Вишег јавног тужилаштва у Београду.

Подаци и документи могу да се сниме и на друге носаче (екстерни хард диск, USB, CD, DVD) од стране овлашћених запослених-корисника.

Носачи информација морају бити прописно обележени и одложени на место на коме ће бити заштуђени од неовлашћеног приступа.

У случају транспорта носача информација, Јавни тужилац ће одредити одговорну особу и начин транспорта.

У случају истека рокова чувања података који се налазе на носачима, подаци морају бити трајно обрисани, ако то није могуће, такви носачи морају бити физички оштећени односно уништени.

Члан 18.

Подаци који се налазе у ИКТ систему представљају тајну у складу са одредбама Закона о слободном приступу информацијама од јавног значаја, Закона о заштити података о личности, Закона о тајности података , као и уредбе о начину и поступку означавања тајности података, односно докумената.

Подаци који се означе као тајни, морају бити заштићени у складу са одредбама уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима.

Документи са ознаком тајности могу да се сниме на друге носаче (екстерни HDD, USB, CD, DVD) само уз сагласност јавног тужиоца Вишег јавног тужилаштва у Београду.

Евиденцију носача на којима се налазе документи са ознаком тајности, води надлежни субјект ИКТ система-систем администратор.

Носачи на којима се налазе документи са ознаком тајности морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта носача са подацима са ознаком тајности, јавни тужилац ће одредити одговорну особу и начин транспорта.

Приликом брисања података са ознаком тајности са носача на којима су се налазили подаци, морају бити неповратно обрисани, а ако то није могуће, такви носачи морају бити физички оштећени, односно уништени.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података.

Члан 19.

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, е маилом, зараженим преносним медијима(USB меморија, CD и итд), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса, на сваком рачунару се инсталира антивирусни програм.

Антивирусни програм у континуитету контролише рачунаре у реалном времену.

Члан 20.

У циљу заштите, односно упада у ИКТ систем Вишег јавног тужилаштва са интернета, систем администратор ВЈТ је дужан да одржава систем за спречавање упада путем интегрисаног система као што је Firewall и Антивирус.

Јавни тужилац Вишег јавног тужилаштва одређује који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за објављање послова у њиховој надлежности

Запослени којима је одобрено коришћење интернета и електронске поште, дужни су да приликом коришћења истог поступају по међународним конвенцијама и правилима понашања.

Запослени којима је одобрено коршћење 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 надлежни систем администратор Вишег јавног тужилаштва.

Приликом коришћења интернета запослени у вишем јавном тужилаштву коме је одобрено коришћење интернета, дужан је да избегава сумњиве web странице, у циљу спречавања инсталирања програма који могу нанети штету ИКТ систему.

У случају да запослени примети необично понашање рачунара, ту појаву је дужан да без одлагања пријави надлежном систем адменистратору.

Члан 21.

Недозвољена употреба интернета обухвата;

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајучи начин:
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;

- намерно ширење деструктивних и опструктивних програма на интернету(интернет вируси, интернет тројански коњ, интернет црви и друга врста недозвољених софтвера)
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено одлуком јавног тужиоца Вишег јавног тужилаштва у Београду;
- преузимање података у количини која проузрокује велико оштећење на мрежи:
- преузимање материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом;
- недозвољен приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

Члан 22.

Заштита од губитка у Вишем јавном тужилаштву у Београду обезбеђује се креирањем резервних делова копија на екстерном диску који је прописно обележен и чува се на обезбеђеном месту.

XII

БЕЗБЕДНОСТ ПОДАТАКА КОЈИ СЕ ПРЕНОСЕ УНУТАР ОПЕРАТОРА ИКТ СИСТЕМА, КАО И ИЗМЕЂУ ОПЕРАТОРА ИКТ СИСТЕМА И ЛИЦА ВАН ОПЕРАТОРА ИКТ СИСТЕМА

Члан 23.

Преносиви медији који садрже податке морају да буду прописано обележени и пописани.

Пренос медија као и начин преноса унутар и ван оператора ИКТ система одређује Јавни тужилац.

Преносиви медији пре стављања ван употребе морају бити физички уништени.

XIII

ПРЕВЕНЦИЈА И РЕАГОВАЊЕ НА БЕЗБЕДНОСТНЕ ИНЦИДЕНТЕ, ШТО ПОДРАЗУМЕВА АДЕКВАТНУ РАЗМЕНУ ИНФОРМАЦИЈА О БЕЗБЕДНОСНИМ СЛАБОСТИМА ИКТ СИСТЕМА, ИНЦИДЕНТИМА И ПРЕТЊАМА

Члан 24.

У случају било каквог инцидента који можда угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести систем администратора Вишег јавног тужилаштва.

По пријему пријаве систем администратор је дужан да о томе обавести Јавног тужиоца и преузме мере заштите ресурса ИКТ система.

Систем администартор води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорних лица, могу да се воде дисциплински, прекршајни или кривични поступци.

ИЗМЕНЕ ПОСТОЈЕЋЕГ И УСПОСТАВЉАЊЕ НОВОГ ИКТ СИСТЕМА

Члан 25.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система, систем администратор Вишег јавног тужилаштва води документацију.

Документација из става 1. овог члана мора да садржи описе свих процедура а посебно процедура које се односе на безбедност ИКТ система.

XIV

ПРОВЕРА ИКТ СИСТЕМА

Члан 26.

Проверу ИКТ система врши систем администратор и информатичар Вишег јавног тужилаштва.

Члан 27.

Провера ће се вршити последњег месеца у години.

Члан 28.

Провера ИКТ система се врши тако што се:

1. проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и акта на који се врши упућивање, са прописаним условима, односно провера да ли су Правилником адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;
2. проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама интервјуа, симулације, посматрања, увида у предвиђене евиденције и другу документацију;
3. врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове) као и методом тестирања постојања постојања познатих безбедносних слабости у сличним окружењима;

О извршеној провери сачињава се извештај који се доставља јавном тужиоцу.

Члан 29.

Извештај из чл 28. овог Правилника садржи:

1. назив оператора ИКТ система који се проверава
2. време провере
3. подаци о лицима која су вршила проверу
4. извештај о спроведенм радњама провере
5. закључке по питању усклађености Акта о безбедности ИКТ система са прописаним условима
6. закључке по питању адекватне примене предвиђених мера заштите у оперативном раду
7. закључке по питању евентуалних слабости на нивоу техничких карактеристика компоненти ИКт система
8. оцене укупног нивоа информационе безбедности
9. предлог евентуалних корективних мера
10. потпис одговорног лица које је спровело проверу ИКТ система(систем администратора).

XV

ПОВРЕДА РАДНЕ ОБАВЕЗЕ

Члан 30.

Непоштовање одредби овог Правилника представља повреду радних обавеза.

Члан 31.

Свако коришћење ИКТ ресурса Вишег јавног тужилаштва у Београду од стране запосленог, ван додељених овлашћења, представља неовлашћено коришћење имовине.

Члан 32.

У случају настанка промена које могу наступити услед техничко технолошких, кадровских, огранизационих промена у ИКТ систему и догађаја на глобалном и националном нивоу, који могу нарушити информациону безбедност, систем администратор је дужан да обавести јавног тужиоца, како би исти могао да приступи измени овог Правилника, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивања овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

XVI

ПРЕЛАЗНЕ И ЗАВРШЕ ОДРЕДБЕ

Члан 33.

Овај Правилник ступа на снагу осмог дана, рачунајући од дана објављивања на огласној табли Вишег јавног тужилаштва у Београду.

У Београду, дана 01.10.2019.године.

ЈАВНИ ТУЖИЛАЦ
ВИШЕГ ЈАВНОГ ТУЖИЛАШТВА
У БЕОГРАДУ
Наташа Кривокапић