Р е п у б л и к а С р б и ј а
ТУЖИЛАШТВО
ЗА РАТНЕ ЗЛОЧИНЕ
А.бр. 201/21
22.10.2021. године
Б е о г р а д
НТ/НЛ

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС” број 6/16, 94/17 и 77/19) у даљем тексту: Закона, члана 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС”, број 94/16), одредбама Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја („Службени гласник РС”, број 94/16), члана 34. Закона о јавном тужилаштву („Сл. гласник РС“ бр. 116/08, 104/09, 101/10, 78/11 – др. закон, 101/11, 38/12 –одлука УС, 121/12, 101/13, 111/14 – одлука УС, 117/14, 106/15 и 63/16 – одлука УС), члана 2. и члана 40. Правилника о управи у јавним тужилаштвима („Сл. гласник РС“ бр. 110/09, 87/10, 5/12, 54/17, 14/18 и 57/19), тужилац за ратне злочине доноси:

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ТУЖИЛАШТВА ЗА РАТНЕ ЗЛОЧИНЕ РЕПУБЛИКЕ СРБИЈЕ

I ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Правилником о безбедности информационо-комуникационог система Тужилаштва за ратне злочине (у даљем тексту: Правилник), у складу са Законом о информационој безбедности („Службени гласник РС”, број 6/16 и 94/17, 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 корисника информатичких ресурса у вези са безбедношћу и ресурсима информационо-комуникационог система Тужилаштва за ратне злочине (у даљем тексту: ИКТ систем).

Члан 2.

Циљеви доношења Акта о безбедности су:

-одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
-спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
-подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
-прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
-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 овим Правилником служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за све запослене-кориснике.

Непоштовање одредаба овог Правилника повлачки дисциплинску одговорност запосленог-корисника информатичких ресурса.

Запослени у Тужилаштву за ратне злочине (у даљем тексту: запослени) морају бити упознати са садржином Правилника и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

За праћење примене овог Правилника надлежан је техничар за ИТ подршку Тужилаштва за ратне злочине.

Члан 4.

Поједини термини у смислу овог Правилника имају следеће значење:

1) ИКТ систем је технолошко-организациона целина која обухвата:

а) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;

б) 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;

в) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачке (а) и (б) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
г) организациону структуру путем које се управља ИКТ системом;

2) 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;

3) тајност је својство које значи да податак није доступан неовлашћеним лицима;

4) интегритет значи очуваност изворног садржаја и комплетности податка;

5) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) 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;

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

8) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

9) 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;

10) инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

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

12) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

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

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

15) криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

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

17) криптографски производ је софтвер или уређај путем кога се врши криптозаштита;

18) криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

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

20) информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

21) Backup је резервна копија података;

22) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;

23) Firewall је „заштитни зид“ односносистем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;

24) USB или флеш меморија је спољшњи медијум за складиштење података;

25) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;

26) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;

Одговорност запослених

Члан 5.

Запослени-корисници 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.

Свако коришћење ИКТ ресурса Тужилаштва за ратне злочине од стране запосленог, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог којом се дефинише одговорност за неовлашћено коришћење имовине.

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 техничар за ИТ подршку Тужилаштва за ратне злочине.

Предмет заштите

Члан 6.

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.

II МЕРЕ ЗАШТИТЕ

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Тужилаштва за ратне злочине, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, коришћења, промене или брисања података, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Члан 7.

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

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

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 Тужилаштва за ратне злочине, надлежан је техничар за ИТ подршку.

Безбедност рада на даљину и употребе мобилних уређаја

Члан 8.

Рад на даљину и употреба мобилних уређаја у ИКТ систему није омогућен.

Члан 9.

ИКТ системом управљају запослени у складу са важећом систематизацијом радних места.

Непосредни руководиоци су дужни да сваког новозапосленог корисника ИКТ система упознају са одговорностима и правилима коришћења ИКТ ресурса Тужилаштва.

Свако коришћење ИКТ ресурса Тужилаштва за ратне злочине од стране запосленог-корисника ван додељених овлашћења, подлеже дисциплинској одговорности.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Члан 10.

У случају промене послова, односно надлежности запосленог-корисника ИКТ система, непосредни руководилац је дужан да обавести техничара за ИТ подршку, односно администратора система, који ће извршити промену привилегија које је запослени имао у складу са описом радних задатака.

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

Носиоци јавнотужилачке функције, запослени и лица ангажована по другом основу дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања, под претњом кривичне и материјалне одговорности.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 11.

Информациона добра су сви ресурси који садрже пословне информације Тужилаштва за ратне злочине у електронском облику или служе за приступ корисника ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију и слично, путем којих се врши израда обрада, чување, пренос, брисање и уништавање података у ИКТ систему.

Тужилаштво врши идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација. Тужилаштво прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води техничар за ИТ подршку у папирној или електронској форми.

Предмет заштите обухвата:

1. хардверске и софтверске компоненте информатичких ресурса;
2. податке који се обрађују или чувају на информатичким ресурсима;
3.корисничке налоге и друге податке о корисницима информатичких ресурса у Тужилаштву за ратне злочине.

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

Члан 12.

Подаци који се налазе у ИКТ систему представљају тајну и као такви морају бити заштићени у складу са одредбама Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. Гласник РС", бр. 53/2011).

Заштита носача података

Члан 13.

Техничар за ИТ подршку ће успоставити организацију приступа и рада са подацима, посебно онима који су од стране управе ТРЗ означени степеном службености или тајности у складу са Законом о тајности података („Службени гласник РС“ бр. 104/09):

-подаци и документи са ознаком тајности снимају се на засебном серверу-рачунару или у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено;

-подаци и документи, као и подаци са ознаком тајности могу да се сниме на друге носаче (екстерни хард диск, УСБ, ЦД, ДВД) само од стране овлашћених запослених корисника.

Евиденцију носача података означених степеном тајности воде овлашћена лица у писарници или кабинету Тужилаштва. Остале евиденције носача података води техничар за ИТ подршку. Сви медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

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 тужиоца за ратне злочине.

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

Носачи информација морају бити прописано обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, тужилац за ратне злочине ће одредити одговорну особу и начин транспорта.

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

Ограничење приступа подацима и средствима за обраду података

Члан 14.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник има.

Запослени који има администраторски налог, има право приступа свим ресурсима ИКТ система (софтверским и хардверским, мрежи и мрежним ресурсима) у циљу инсталације, одржавања, подешавања и управљања ресурсима ИКТ система.

Запослени-корисник може да користи 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-корисник који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.

Запослени-корисник дужан је да поштује и следећа правила безбедног и примерног коришћења ресурса ИКТ система и то да:

1. користи информатичке ресурсе искључиво у пословне сврхе;
2. прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Тужилаштва за ратне злочине;
3. поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. безбедно чува своје лозинке, односно да их не одаје другим лицима;
5. мења лозинке сагласно утврђеним правилима;
6. пре сваког удаљавања од радне станице, одјави се са система, односно закључа радну станицу;
7. захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
8. обезбеди сигурност података у складу са важећим прописима;
9. приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
10. не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11. на радној станици не сме да складишти садржај који не служи у пословне сврхе;
12. израђује заштитне копије података у складу са прописаним процедурама;
13. користи интернет и електронску пошту у складу са прописаним процедурама;
14. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
15. прихвати да технике сигурности (антивирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;

16. не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 15.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља.

Право приступа имају запослени-корисници који имају администраторске или корисничке налоге. Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Администраторски налог може да користи искључиво систем-администратор, односно техничар за ИТ подршку Тужилаштва за ратне злочине.

Администратор додељује кориснички налог на основу захтева запосленог задуженог за кадровске послове, у сарадњи са непосредним руководиоцем, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

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.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева запосленог на кадровским пословима, односно надлежног руководиоца.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 16.

Аутентификација корисника којима је одобрен приступ систему врши се путем јединственог корисничког налога који се састоји од имена и лозинке.

Корисничко име се креира латиничним писмом по матрици име.презиме.

Уколико два корисника имају исто име и презиме, између се додаје средње слово или више, одвојено тачкама.

Лозинка мора да садржи минимум седам карактера, састављених комбинацијом латиничних великих и малих слова, цифара и специјалних знакова.

Запослени-корисник дужан је да мења лозинку једном у годину дана или чешће када то систем захтева од њега, након истека системски подешеног периода за промену лозинке.

Ако запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

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

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

Члан 17.

Приступ ресурсима ИКТ система Тужилаштва за ратне злочине не захтева посебну криптозаштиту.

Запослени-корисници које тужилачка управа или непосредни руководилац одреди, користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама и порталима ван Тужилаштва, сходно радним задацима које обављају.

Запослени на пословима ИКТ су задужени за инсталацију потребног софтвера и хардвера за коришћење сертификата.

Запослени-корисници су дужни да чувају своје квалификоване елетронске сертификате како не би дошли у посед других лица.

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

Члан 18.

Тужилаштво за ратне злочине је дужно да предузме мере ради спречавања неовлашћеног физичког приступа просторијама у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација и опреме за обраду информација.

Простор треба да буде обезбеђен од компротимујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода и у њему треба да буде одговарајућа температура (климатизован простор).

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

Члан 19.

Улаз у сервер салу (просторију у којој се налази ИКТ опрема) дозвољен је само овлашћеним лицима у Тужилаштву за ратне злочине.

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

Осим овлашћених лица у Тужилаштву за ратне злочине, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу управе Тужилаштва или надлежног руководиоца и уз присуство једног запосленог из ИТ сектора.

Приступ административној зони може имати и запослени на пословима одржавања хигијене, уз присуство запосленог лица из ИТ сектора.

Просторија мора бити обележена и у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима.

Прозори и врата на овој просторији морају бити затворени.

Сервери и активна мрежна опрема (switch, modem, router, firewall) морају стално бити прикључени на уређаје за непрекидно напајање – UPS.

У случају нестанка електричне енергије, у периоду дужем од капацитета UPS-а, овлашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења управе Тужилаштва за ратне злочине.

У случају изношења опреме ради селидбе или сервисирања, неопходно је одобрење тужиоца за ратне злочине који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, потребно је сачинити реверс у коме се наводи назив и тип опреме, серијски број и назив сервисера, који потписује техничар за ИТ подршку.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 20.

Техничар за ИТ подршку континуирано надзире и проверава функционисање средстава за обраду података и управља ризицима који могу утицати на безбедност ИКТ система и у складу са тим планира и предлаже тужиоцу за ратне злочине одговарајуће мере.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију.

Инсталирање новог софтвера, као и ажурирање постојећег, односно инсталација нове верзије, може се вршити на начин који не омета оперативни рад запослених-корисника.

У случају да се на новој верзији софтвера који је уведен у оперативни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

За развој и тестирање софтвера пре увођења у рад у ИКТ систем морају се користити сервери и подаци који су намењени тестирању и развоју.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 21.

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 меморија, CD, итд.), инсталацијом нелиценцираног софтвера и сл.

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 информационе безбедности, као и на одговарајућим контролама приступа систему и управљању захтеваним и потребним променама.

За успешну заштиту од вируса на сваком рачунару инсталиран је антивирусни програм.

Свакодневно се аутоматски врши допуна антивирусних дефиниција.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером.

Ризик од евентуалног губитка података приликом чишћења медија од вируса сноси доносилац медија.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави техничару за ИТ подршку.

Тужилац за ратне злочине одређује ниво приступа интернету сходно потребама посла.

Корисници ИКТ система који користе интернет на рачунарима морају 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 техничар за ИТ подршку.

Приликом коришћења интернета треба избегавати сумњиве WEB странице, с обзиром да то може проузроковати проблеме – неприметно инсталирање шпијунских програма и слично.

Корисницима који на неадекватан начин користе интернет и тако узрокују загушење, прекид у раду или нарушавају безбедност мреже, може се одузети право приступа интернету.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема).

Заштита од губитка података

Члан 22.

Заштита од губитка података у Тужилаштву за ратне злочине обезбеђује се креирањем резервних копија на екстерном диску који је прописно обележен и чува се на обезбеђеном месту. Сви документи штампани из ИКТ система се меморишу као ПДФ (PDF) или доц (doc ili docx) документи.

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

Члан 23.

У ИКТ систему Тужилаштва за ратне злочине формирају се записи (логови) о активностима администратора и запослених - корисника, грешкама и догађајима у вези са информационом безбедношћу.

Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

Тужилаштво за ратне злочине спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система у складу са смерницама за контролу промена и инсталацију софтвера.

Инсталацију и подешавање софтвера врши техничар за ИТ подршку.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера, уз присуство запосленог техничара за ИТ подршку.

Пре сваке инсталације нове верзије софтвера, односно подешавања, неопходно је направити копију постојећег, како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 25.

Техничар за ИТ подршку подешава корисничке полисе у циљу спречавања неовлашћеног инсталирања софтвера који може довести до угрожавања безбедности ИКТ система и по потреби прати и анализира дневник активности у циљу идентификације потенцијалних слабости ИКТ система.

Уколико се идентификују слабости које могу да узрозе безбедност ИКТ система, систем администратор је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

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

Члан 26.

Приликом спровођења ревизије ИКТ система Тужилаштво обезбеђује да ревизија ИКТ система има што мањи утицај на послове корисника-запослених и на функционисање система.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 27.

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, firewall) се мора налазити у закључаном rack орману.

Техничар за ИТ подршку је дужан да врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

У циљу заштите података у комуникационим мрежама, уређајима и водовима врши се њихова контрола и заштита од неовлашћеног приступа.

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

Члан 28.

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 29.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Тужилаштву за ратне злочине, дефинише се уговором склопљеним са тим лицима.

Техничар за ИТ подршку задужен је за надзор над реализацијом уговорених обавеза од стране трећих лица.

Документацију, упутства и процедуре добијене од трећих лица при инсталацији или замени ресурса ИКТ система чува техничар за ИТ подршку.

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

Члан 30.

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 упоредила актуелна и очекивана понашања.

За потребе тестирања могу се користити само оперативни подаци који нису осетљиви.

Приликом тестирања система не могу се користити подаци који представљају податке о личности, нити подаци који су под ознаком тајности, односно службености као поверљиви подаци.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 31.

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 32.

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

За надзор над поштовањем уговорених обавеза од стране трећих лица, задужен је техничар за ИТ подршку који је у случају непоштовања тих обавеза, дужан да о томе одмах обавести кабинет Тужилаштва.

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

Члан 33.

Тужилац за ратне злочине одређује техничара за ИТ подршку да, придржавајући се процедура одређених овим чланом, планира, детектује, анализира и информише надлежне у току и након инцидента.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система Тужилаштва, запослени-корисник је дужан да о томе одмах обавести техничара за ИТ подршку.

У зависности од врсте и значаја инцидента, техничар за ИТ подршку је дужан да одмах предузме мере у циљу заштите ресурса ИКТ система и да о томе обавести Управу Тужилаштва.

Техничар за ИТ подршку води евиденцију о инцидентима, као и пријавама инцидената, у складу са уредбом на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 34.

Тужилаштво за ратне злочине примењује мере које обезбеђују континуитет обављања посла у ванредним околностима како би ИКТ систем био у што краћем року у функционалном стању.

Провера ИКТ система

Члан 35.

Проверу ИКТ система врши техничар за ИТ подршку Тужилаштва за ратне злочине или друго овлашћено лице.

Обавеза Тужилаштва је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене овог Правилника, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Тужилаштва за ратне злочине.

Провера се врши тако што се проверава усклађеност Правилника о безбедности ИКТ система, узимајући у обзир и правилнике на које се врши упућивање, са прописаним условима, односно проверава да ли су Правилником адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему; да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима; 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 познатих безбедносних слабости у сличним окружењима.

О извршеној провери сачињава се извештај који се доставља секретару Тужилаштва.

Измена Правилника о безбедности

Члан 36.

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, техничар за ИТ подршку је дужан да обавести секретара Тужилаштва и тужиоца за ратне злочине, како би они могли да приступе измени овог акта, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу ресурса ИКТ система.

III САДРЖАЈ ИЗВЕШТАЈА О ПРОВЕРИ ИКТ СИСТЕМА

Члан 37.

Извештај о провери ИКТ система садржи:

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

IV ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Ступање на снагу Правилника о безбедности

Члан 38.

Овај Правилник ступа на снагу даном доношења, а његова примена отпочиње по истеку рока од 8 (осам) дана од дана објављивања на огласној табли Тужилаштва за ратне злочине.