Република Србија
ДРЖАВНО ПРАВОБРАНИЛАШТВО
Број: II Дп-760/19
01. август2019. године
Београд
Немањина 26

На основу члана 8. Закона о информационој безбедности („Службени гласник РС“, број 6/16 и 94/17), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо-комукационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комукационог система од посебног значаја („Сл. гласник РС“, бр. 94/2016) Државни правобранилац је донео

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО – КОМУНИКАЦИОНОГ СИСТЕМА ДРЖАВНОГ ПРАВОБРАНИЛАШТВА

I. Уводне напомене

Члан 1.

Овим правилником, у складу са Законом о информационој безбедности и Уредбом о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начин провере информационо-комуникационих система од посебног значаја и садржај извештаја о провери информационо-комукационог система од посебног значаја („Сл. Гласник РС“, бр. 94/2016), утврђују се 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 информационо-комуникационог система Државног правобранилаштва.

Члан 2.

Мере прописане овим правилником се односе на све организационе целине Државног правобранилаштва, на све запослене/кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Државног правобранилаштва.

Непоштовање одредби овог правилника повлачи дисциплинску одговорност запосленог/корисника информатичких ресурса.

Сви запослени дужни су да поступају у складу са одредбама овог Правилника, као и других интерних процедура које регулишу информациону безбедност.

II Мере заштите

Члан 3.

Мерама заштите ИКТ система Државног правобранилаштва се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Приликом планирања и примена мера заштите ИКТ система треба се руководити начелима свеобухватне заштите, стручности и способности управљања ризицима.

Мере заштите ИКТ система, прописане овим Правилником, односе се на.

1. Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којиом се остварује управљање информационом безбедношћу у оквиру Државног правобранилаштва,
2. Постизање безбедности рада на даљину и употребе мобилних телефона,
3. Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који обављају и разумеју своју одговорност
4. Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених у Државном правобранилаштву
5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту
6. Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој безбедности
7. Заштиту носача података
8. Ограничење приступа подацима и средствима за обраду података
9. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа
10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

11. Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података
12. Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему
13. Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем
14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података
15. Заштиту података и средства за обраду података од злонамерног софтвера
16. Заштиту од губитка података
17. Обезбеђивање интегритета софтвера и оперативних система
18. Заштита од злоупотребе безбедносних слабости ИКТ система
19. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система
20. Заштиту података у комуникационим мрежама укључујући уређаје и водове;
21. Безбедност података који се преносе унутар Државног правобранилаштва, као и између Државног правобранилаштва и лица ван Државног правобранилаштва;
22. Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;
23. Заштиту података који се користе за потребе тестирања ИКТ система односно делова система;
24. Заштиту средстава Државног правобранилаштва која су доступна пружаоцима услуга;
25. Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;
26. Превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама;

Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Државног правобранилаштва

Члан 1.

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

Интерни акти који уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу су:

-Правилник о безбедности информационо – комуникационог система Државног правобранилаштва;

-Правилник о унутрашњем уређењу и систематизацији радних места у Државном правобранилаштву;

-Решења о распоређивању;

-Уговори о раду;

-Изјаве о поверљивости;

-Уговори о чувању поверљивости са правним лицима.

Сваки запослени/корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова из своје надлежности, у складу са постојећом систематизацијом радних места у Државном правобранилаштву.

Члан 5.

Под пословима из области безбедности утврђују се:

- Послови заштите информационих добара, односно средства и имовине за надзор на пословним процесима од значаја за информациону безбедност;
- Послови управљања ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедности;
- Послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Државног правобранилаштва, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе;
- Праћење активности, ревизије и надзора у оквиру управања информационом безбедношћу;
- Обавештавање надлежних органа о инцидентима у ИКТ систему, у складу са прописима.

У случају инцидента корисник информатичких ресурса је дужан да, у циљу решавања насталог безбедносног инцидента, без одлагања, инцидент пријави непосредном руководиоцу и руководиоцу Групе за информатику и аналитику.

Безбедност рада на даљину и употреба мобилних уређаја

Члан 6.

Нерегистровани корисници, путем мобилних уређаја могу да приступе само оним деловима мреже који су конфигурисани тако да омогућавају приступ интернету али не и деловима мреже кроз коју се обавља службена комуникација.

Запосленом/кориснику, забрањена је самостална инсталација софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима (на услугу, сервисирање и сл.)

Приватни уређаји са којих ће се приступати ресурсима ИКТ система морају бити подешени од стране Групе за информатику и аналитику.

Коришћење мобилних уређаја

Мобилни уређаји подразумевају све преносне електронске уређаје намењене за комуникацију на даљину. У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони, и сви други мобилни уређаји који садрже податке и имају могућност повезивања на мрежу.

Процедуром о коришћењу мобилних уређаја дефинише се начин физичке заштите од крађе и активности које је неопходно предузети у случају крађе или губитка мобилних уређаја.

Процедура о коришћењу мобилних уређаја је следећа:

1. Сви уређаји морају бити заштићени јаком шифром,
2. Инсталирана је антивирусна заштита,
3. Подаци за чијим чувањем је престала потреба се бришу по процедури за потпуно брисање,
4. Крађа или губитак мобилног уређаја се мора без одлагања пријавити Секретаријату - Групи за информатику и аналитику и Групи за финансијско-материјално пословање,
5. Корисницима није дозвољено да врше измене на хардверу или инсталираном софтверу који је власништво Државног правобранилаштва без претходне писане дозволе руководиоца органа,

Процедура из претходног става се примењује на запослене на неодређено време, запослене на одређено време и лица ангажована по другим основама, која имају приступ или користе мобилне уређаје у власништу ИКТ система Државног правобранилаштва.

Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који обављају и разумеју своју одговорност

Члан 8.

Државно правобранилаштво 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. Одговорности су утврђене

решењем о распоређивању и Правилником о унутрашњем уређењу и систематизацији радних места у Државном правобранилаштву.

У циљу провере испуњености услова сваког појединачног кандидата приликом пријема у радни однос врши се провера компетенција за свако радно место у складу са Уредбом о одређивању компетенција за рад државних службеника и Правилником о посебним функционалним компетенцијама за запослене у судовима, јавним тужилаштвима и Државном правобранилаштву.

Сви запослени и радно ангажовани појединци по другом основу којима је додељен приступ поверљивим информацијама, морају потписати изјаву о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Запослени у Групи за информатику и аналитику континуирано се обучавају у циљу унапређења техничког и технолошког знања.

Ова лица су ауторизована за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

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

Свако коришћење ИКТ ресурса Државног правобранилаштва од стране запосленог/корисника, ван додељених овлашћења, подлеже дисциплинској одговорности запосленог за неовлашћено коришћење имовине.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених у Државном правобранилаштву

Члан 9.

У случају промене послова, односно надлежности корисника/запосленог, Група за информатику и аналитику ће извршити промену привилегија које је корисник/запослени имао у складу са описом радних задатака, а на основу захтева непосредног руководиоца и/или Групе за правне и кадровске послове.

У случају престанка радног ангажовања корисника/запосленог, кориснички налог се проглашава неактивним.

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

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра Државног правобранилаштва обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре који се односе на ИКТ систем и сл.

Предмет заштите су:

- Хардверске и софтверске компоненте ИКТ система
- Подаци који се обрађују или чувају на компонентама ИКТ система
- Кориснички налози и други подаци о корисницима информатичких ресура ИКТ система.

Евиденцију о информационим добрима води Група за информатику и аналитику и Група за финансијско-рачуноводствене послове.

Група за финансијско-рачуноводствене послове упућује захтев, Управи за заједничке послове републичких органа са доказом о начину стицања, ради уписа наведеног купљеног односно прибављеног добра у Листу основних средстава.

Група за информатику и аналитику води евиденцију о праву коришћења добара, које је додељено кроз пратећу документацију-задужење.

Једном годишње врши се попис добара по процедури у складу са Законом о рачуноводству и Закону о буџетском систему.

Запослени и екстерни корисници су обавезни да врате сву имовину Државног правобранилаштва коју користе након престанка рада, односно основа ангажовања.

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

Члан 11.

Класификовање података се врши ради:

- Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност података приликом чувања или слања и буду свесни одговорности за неовлашћено коришћење или преношење;
- Подизања свести о вредности информације или документа;

- Заштите података у покрету ради боље и интелигентније интеграције са DLP, WEB gateway и осталим производима за заштиту параметара и крајњих уређаја;
- Заштите садржаја;
- Интеграције са системима за архивирање.

Подаци које се налазе у ИКТ систему Државног правобранилаштва, представљају тајну, ако су тако дефинисани одредбама и посебним прописима[1].

Подаци који се означе као тајни, 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 12.

Спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података обезбеђује Канцеларија за информационе технологије и електронску управу, ИТЕ (у даљем тексту: надлежни субјект ИКТ система)

Група за информатику и аналитику у сарадњи са ИТА ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном тајности у складу са Законом о тајности података, тако да:

- подаци и документи (посебно они са ознаком тајности) 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 руководиоца органа
- подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, USB, CD, DVD) само од стране овлашћених запослених/корисника.

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

[1] Закон о слободном приступу информацијама од јавног значаја („Сл. Гласник РС“, бр. 120/04, 54/07, 104/0*9 и 36/10), Закон о заштити података о личности („Сл. гласник РС“, бр. 97/08, 104/09-др. Закон 68/12, - ОДЛУКА УС и 107/2012), Закон о тајности података („Сл. гласник РС“, 104/20019), као и Уредба о начину и поступку означавања тајности података, односно докумената („Сл. гласник РС“, бр. 8/2011)

Ограничење приступа подацима и средствима за обраду података

Члан 13.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени-корисник 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/ 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 примереног 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 процесуирају у оквиру информатичких ресура власништво Државног правобранилаштва и да могу бити предмет надгледања и прегледања
3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података
4) безбедно чува своје лозинке,
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,
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) израђује заштитне копије (backup) података у складу са чланом 23. Правилника,
12) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време,
13) прихвати да техничке сигурности (антивирусни програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему,
14) 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 14.

Право приступа имају само 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/могу да користе само запослени на пословима ИТ Државног правобранилаштва.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу кога 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 обавештења Групе за правне и кадровске послове путем е-маила, а којим се информише администратор, о пријему у радни однос односно радном ангажовању новог запосленог /корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу информација које администратор добија од Групе за правне и кадровске послове о пријему у радни однос односно раскиду уговора о радном ангажовању лица.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15.

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

Сви корисници су дужни да:

- избегавају чување корисничког имена и шифре>у писаном облику;
- промене шифру увек када постоји било какав наговештај могућег компромитовања.

Шифре треба да садрже:

- најмање 9 алфанумеричких карактера
- најмање једно велико и једно мало слово

- најмање 1 број (0-9).

Шифре не смеју бити засноване на подацима-карактерима који лако могу бити откривени од неовлашћеног лица.

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

Члан 16.

Приступ ресурсима ИКТ система Државног правобранилаштва не захтева посебну криптозаштиту.

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

Члан 17.

Смештај серверске опреме Државног правобранилаштва, у државни Дата центар и коришћење виртуелних сервера у државном Дата центру, који се налази у Београду, односно услугу Telehausinga.обавља, ИТЕ.

Физичку заштиту објекта у седишту органа, Немањина 22-26 пружа Министарство унутрашњих послова.

Физичку заштиту објекта Палата Србије у којој је смештено Одељење за заступање Републике Србије пред Европским судом за људска права пружа Министарство унутрашњих послова.

Државно правобранилаштво планира и примењује инструменте за обезбеђивање физичке заштите објеката у које су смештена Одељења, на иницијативу заменика државног правобраниоца који руководи одељењем, на начин да се онемогућава јавни приступ кључној опреми.

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

Члан 18.

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења.

Просторија мора бити видљиво 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 увек бити затворени.

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

ИКТ опрема из просторије се у случају опасности (пожар, временске непогоде и сл.) може изнети и без одобрења непосредног руководиоца.

У случају изношења опреме из седишта органа, ради селидбе или сервисирања, неопходно је одобрење секретара.

Ако се опрема износи ради сервисирања, Група за информатику и аналитику припрема допис којим се обавештава обезбеђење зграде о изношењу опреме, а који садржи назив и тип опреме, серијски број, као и назив сервисера, и када је познато и име и презиме овлашћеног лица сервисера.

Остављање осетљивих и поверљивих докумената и материјала

Члан 19.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

Процедура:

1. Све осетљиве и поверљиве информације у штампаном или електронском облику запослени морају одложити на сигурно место на крају радног дана или када нису присутни на свом радном месту;
2. Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана;
3. Ормари и фиоке у којима се чувају поверљиви подаци морају бити закључани када се не користе, а кључеви не смеју бити остављени на приступачном месту без надзора;
4. Лаптопови морају бити везани уз помоћ одговарајуће опреме или закључани у фиоци. Таблети и остали преносни уређаји морају бити закључани у фиоци;
5. Носиоци података као што су дискови и flash меморија морају бити одложени и закључани;
6. Шифре за приступ не смеју бити написане и остављене на приступачном месту;

7. Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.

Материјал који је намењен за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 20.

Запослени на пословима ИКТ проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и у складу са тим, предлажу одговарајуће мере.

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

При тестирању софтвера је потребно обезбедити неометано функционисање ИКТ система.

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

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

Заштита података и средства за обраду података од злонамерног софтвера

Члан 21.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен или неумрежен рачунар.

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

За успешну заштиту од вируса на сваком рачуну је инсталиран 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.

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

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем.

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

У случају да корисник примети необично понашање рачунара, запажање се без одлагања, пријављује Групи за информатику и аналитику.

Строго је забрањено гледање филмова и играње игрица на рачунарима и „крстарење“ WEB страницама које садрже недоличан садржај, као и самовољно преузимање истих са интернета.

Члан 22.

Недозвољена употреба интернета обухвата и:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских“ или других софтверских производа који нису лиценцирани на одговарајући начин;
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено одлуком државног правобраниоца;
- преузимање (download) података велике „тежине“ које проузрокује „загушење“ на мрежи
- преузимање (download) материјала заштићених ауторским правима
- забрањено је гледање филмова, аудио и videostreaming и сл.
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

Заштита од губитка података

Члан 23.

Када постоји потреба, базе података се архивирају на преносиве медије (CDROM, DVD, USB, „strimer“ трака, екстерни хард диск), најмање једном у шест месеци или по потреби чешће.

Обезбеђивање интегритета софтвера и оперативних система

Члан 24.

У ИКТ систему се инсталира само софтвер за који постоји важећа лиценца у власништву Државног правобранилаштва, односно бесплатан софтвер (енг. Freeware) и софтвер отвореног кода (енг.Open Source верзије).

Инсталацију и подешавање софтвера врши надлежни субјект ИКТ система и/или Група за информатику и аналитику односно запослени-корисник који има овлашћење за то.

Инсталацију и подешавање софтвера може да изврши и треће лице, у случају када је софтвер набављен у поступку јавне набавке, у складу са Уговором о набавци.

Треће лице може да изврши инсталацију и подешавање софтвера када је између Државног правобранилаштва и трећег лица уговорено одржавање софтвера.

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 безбедносних слабости ИКТ система

Члан 25.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, надлежни субјект ИКТ система и/или Група за информатику и аналитику одмах врши подешавања, односно инсталира софтвер који ће отклонити уочене слабости.

Надлежни субјект ИКТ система и/или Група за информатику и аналитику, онемогући неовлашћено инсталирање софтвера који може довести до угрожавања безбедности ИКТ система.

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

Члан 26.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника/запослених.

Уколито то није могуће у радно време, ревизија ИКТ система се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну салгасност надређених.

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 неоволашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, router, firewall) треба да се налази у закључаном rack орману.

Када се укаже потреба за предузимањем мера у циљу отклањања евентуалних неправилности, запослени-корисник обавештава Групу за информатику и аналитику која у сарадњи са надлежним субјектом ИКТ система врши контролни преглед мрежне опреме и предузима мере у циљу отклањања неправилности.

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

Члан 28.

Размена података са заступаним органима у апликацији за електронско вођење предмета Државног правобранилаштва Лурис који се користи за вођење евиденције о предметима и у вези са предметима у седишту органа, врши се преко одређених официра за везу.

Одржавање апликације је у надлежности трећег лица на основу Уговора о одржавању у одређеном временском периоду.

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 Државном правобранилаштву дефинише се међусобно закљученим уговором.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система документацију води Група за информатику и аналитику.

Надлежни субјект ИКТ система и/или Група за информатику и аналитику је задужен/а за надзор над реализацијом уговорених обавеза са трећим лицима.

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

Члан 30.

Приликом тестирања ИКТ система, надлежни субјект ИКТ система и Група за информатику и аналитику одговара за податке у складу са прописима којима је дефинисана употреба и заштита такве врсте података - подаци који су означени ознаком тајности, односно службености као поверљиви подаци или су лични подаци.

Заштита средстава ИКТ система која су доступна пружаоцима услуга

Члан 31.

Трећа лица-пружаоци услуга израде и одржавања софтвера могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили, односно за које постоји уговором дефинисан приступ.

Група за информатику и аналитику је одговорна за контролу приступа и надзор над извршењем уговорених обавеза које је Државно правобранилаштво закључило са трећим лицима у области унапређења апликације.

Члан 32.

Надлежни субјект ИКТ система је одговоран за надзор над поштовањем уговорених обавеза од стране трећих лица-пружаоца услуга, посебно у области поштовања одредби којима је дефинисана безбедност ресурса ИКТ система.

У случају непоштовања уговорених обавеза надлежни субјект ИКТ система је дужан да одмах обавести секретара и руководиоца Групе за информатику и аналитику.

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

Члан 33.

Државно правобранилаштво има склопљен уговор са трећим лицима за пружање услуга информационе безбедности.

У случају непоштовања уговорених обавеза Група за информатику и аналитику је дужна да обавести секретара ради предузимања мера у циљу отклањања неправилности.

Превенција и реаговање на безбедносне инциденте

Члан 34.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени/корисник је дужан да одмах обавести Групу за информатику и аналитику.

По пријему пријаве из става 1.овог члана, Група за информатику и аналитику је одмах предузме мере у циљу заштите ИКТ система.

Члан 36.

Уколико се ради о инциденту који је дефинисан Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, надлежни субјект ИКТ је дужан да поред државног правобраниоца обавести и надлежни орган дефинисан наведеном Уредбом.

Група за информатику и аналитику води евиденцију о инцидентима, као и пријавама инцидената, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни и кривични поступци.

IV ПРОВЕРА ИКТ СИСТЕМА

Члан 37.

Проверу ИКТ система врши надлежни субјект ИКТ система и Група за информатику и аналитику.

Проверу ИКТ система може вршити и лице изабрано у складу са законом који се уређује поступак јавних набавки.

Провера ИКТ система се врши тако што се:

1. проверава усклађеност Правилника о безбедности ИКТ система у Државном правобранилаштву узимајући у обзир и акта на које се врши упућивање, са прописаним условима,
2. проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама интрвјуа, 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, техничке конфигурације, записе о догађајима .

О извршеној провери сачињава извештај, који се доставља државном правобраниоцу на захтев.

V САДРЖАЈ ИЗВЕШТАЈА О ПРОВЕРИ ИКТ СИСТЕМА

Члан 38.

Извештај о провери ИКТ система садржи:

1) назив оператора ИКТ система који се проверава;
2) време провере;
3) подаци 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 компоненти ИКТ система;
8) оцена укупног нивоа информационе безбедности;
9) предлог евентуалних корективних мера;
10) потпис одговорног лица које је спровело проверу ИКТ система.

VI ДИСЦИПЛИНСКА ОДГОВОРНОСТ

Члан 39.

Непоштовање одредби овог Правилника представља повреду радних обавеза и повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса Државног правобранилаштва.

Члан 40.

Свако коришћење ИКТ ресурса Државног правобранилаштва од стране запосленог-корисника, ван додељених овлашћења подлеже дисциплинској одговорности запосленог којим се дефинише одговорност за неовлашћено коришћење имовине.

Члан 41.

Корисницима који неадекватним коришћењем интернета узрокују загушење, прекид у раду или нарушавају безбедност мреже, може се одузети право приступа.

VII ИЗМЕНА ПРАВИЛНИКА

Члан 42.

У случају настанка промене које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, Група за информатику и аналитику је дужна да обавести Државног правобраниоца, како би он могао да приступи измени овог правилника, 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 и ресурсима ИКТ система.

ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 43.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли Државног правобранилаштва.

Државни правобранилац

Оливера Станимировић