На основу члана 23. став 2. Закона о државној управи („Службени гласник РС”, број 79/05, 101/07, 95/10, 99/14, 47/18 и 30/18 – др. закон), а у вези члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16 и 94/17), чл. 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), Министар правде доноси

Акт о безбедности информационо-комуникационог система

Министарства правде и органа у саставу

I. ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система Министарства правде и органа у саставу (у даљем тексту: Акт о безбедности), 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 у вези са безбедношћу и ресурсима информационо-комуникационог система Министартсва правде и органа у саставу (у даљем тексту: ИКТ систем).

Саставни део Акта о безбедности информационо-комуникационог система су директиве које одређују начин рада, понашање запослених у области информационе безбедности, као и интерне процедуре, прописане овим актом, које су одштампане уз овај акт, и чине његове прилоге.

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

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

Запослени у Министарству правде и органа у саставу (у даљем тексту: Министарства правде) морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

Сектор за материјално-финансијске послове правде одговоран је за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност запослених

Члан 4.

Запослени у Министарству правде су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим безбедносним инцидентима и проблемима.

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

Предмет заштите

Члан 5.

Мере заштите ИКТ система односе се на заштиту информциоих добара. Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично;.

Министарство правде је извршило попис и идентификацију своје информационе имовине коју жели да заштити, у оквиру **Регистра информационе имовине** у којем се врши опис основних средстава и друге опреме у виду комплетне евиденције задужене опреме за сваког запосленог. Ова евиденција представља подскуп евиденције која се успоставља у оквиру редовног поступка пописа имовине и обавеза за сваку календарску годину. Овај попис спроводе комисије за попис имовине и обавеза које се образују решењима. Попис имовине и обавеза регулисан је Уредбом о буџетском рачуноводству, Уредбом о евиденцији и попису непокретности и других средстава у државној својини и Правилником о начину и роковима вршења пописа и усклађивања књиговодственог стања са стварним стањем.

II. МЕРЕ ЗАШТИТЕ

Сваки члан садржи опис мера заштите укључујући предлоге процедура, овлашћења и одговорности учесника у спровођењу мера. Уколико су ти описи садржани у другим актима оператора ИКТ система наведене су одредбе које упућују на та акта.

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

Члан 6.

Министарство правде у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

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

- Правилник о унутрашњем уређењу и систематизацији радних места у Министарству правде;
- Уговори о раду;
- **Споразум о поверљивости и неоткривању за физичка лица - НДА**;
- **Споразум о поверљивости и неоткривању за правна лица - НДА**;

СМФ је дужан да у оквиру уговора о раду, у складу са актом о систематизацији, одређује одговорна лица за заштиту информационог система и праћење информационе безбедности у Министарству правде. Сви запослени морају бити упознати са Актом о безбедности ИКТ система Министарства правде.

Министарство правде у оквиру **Процедуре за употребу ИКТ опреме и поступање са информацијама**, **Процедуре за контролу приступа**, **Упутства за мрежну безбедност** и **Процедуре за удаљени приступ** утврђује начин доделе овлашћења за приступ ИКТ систему, начин одобравања приступа запосленима од стране руководиоца, односно непосредно надређеног лица. **Правилником процене вештина запослених и потребе за обуком**, **Упитником о вештинама** и **Упитником о вештинама - анализа одговора** организација утврђује степен обуке и квалификацију запослених.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 7.

Министарство правде дозвољава рад на даљину и употребу мобилних уређаја од стране запослених, уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја.

Рад на даљину

Члан 8.

Радни однос за обављање послова ван просторија послодавца обухвата:

- Рад на даљину;
- Рад од куће;
- Виртуелно радно окружење.

Предметно ангажовање и омогућавање обављања задатих и неопходних послова се уређује уз коришћење **Водича за безбедан рад од куће** (акт Министарства за рад, запошљавање, борачка и социјална питања) и путем **Процедуре за контролу приступа**, **Упутства за мрежну безбедност** и **Процедуре за удаљени приступ** у оквиру којих је описан процес за VPN приступ информационом систему.

Такође, рад на даљину у смислу овог Акта односи се на ситуацију када је запослени и други радно ангажовани обавезан да изврши одређене послове на мрежи послодавца, а налази се ван просторија послодавца.

Предметно ангажовање и омогућавање обављања задатих и неопходних послова се уређује путем Упутства за мрежну безбедност и Процедуре за удаљени приступ. VPN приступ дефинише правила и услове за повезивање на мрежу Министарства правде са удаљене локације. Правилном применом утврђеног поступка и начина приступа, Министарство своди на минимум

потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи. VPN приступ се примењује на све запослене у Министарству правде и сараднике који користе рачунаре или мобилне уређаје за повезивање на мрежу, и уређује приступ са удаљених локација у сврху обављања посла у име и за рачун Министрства правде, укључујући коришћење електронске поште и мрежних ресурса, као и начин приступа мрежи са удаљених локација.

Ауторизованим корисницима није дозвољено да користе мрежу Министрства правде за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада појединачно запосленог.

Захтеви који морају бити испуњени и дефинисани приликом VPN приступа:

1. Приступ са удаљених локација мора бити заштићен коришћењем криптографских алгоритама.
2. Ауторизовани корисници морају чувати креденцијале својих налога и не смеју омогућити приступ било ком трећем лицу.
3. Приликом коришћења службеног рачунара за приступ са удаљене локације мрежи Министарства правде, ауторизовани корисник не сме истовремено бити повезан и на неку другу мрежу која може угрозити безбедност комуникације.
4. Приступ са удаљене локације мора бити одобрен од стране одговорног лица за надзор спровођења VPN приступа.
5. Сви уређаји који су повезани на интерну мрежу преко удаљених локација морају имати инсталирану заштиту у виду антивирусног софтвера.
6. Сви пословни подаци који се креирају приликом рада на даљину складиште се у информационом систему. Ради безбедности, пословни подаци се не складиште на мобилним уређајима.

Рад на даљину запослених или других радно ангажованих (ангажованих за рад у просторијама послодавца) одобрава Сектор за материјално-финансијске послове Министарства.

Коришћење мобилних уређаја

Члан 9.

Мобилни уређаји подразумевају све преносне електронске уређаје намењене за комуникацију на даљину. У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони, PDA и сви други мобилни уређаји који садржи податке и имају могућност повезивања на мрежу. Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Директивом о коришћењу преносивих уређаја и бежичних веза дефинише се начин физичке заштитите од крађе и активности које је неопходно предузети у случају крађе или губитка мобилних уређаја, односно безбедносног инцидента, како не би била нарушена безбедност.

Министарство правде спроводи обуку запослених који користе мобилне уређаје, у циљу подизања свести о додатним ризицима до којих долази услед оваквог начина рада.

Упутством за безбедност преносивих уређаја установљена су следећа правила:

1. Сви уређаји морају бити заштићени јаком шифром.
2. Мора бити инсталирана антивирусна заштита.

3. Мора бити усвојена и оперативна процедура за потпуно брисање података када престаје потреба за чувањем истих.
4. Крађа или губитак мобилног уређаја се мора без одлагања пријавити СМФу и одговорном лицу из службе за ИТ, који затим спроводе активности у смислу очувања безбедности. Уколико се уређај пронађе, потребно је предати исти одговорним лицима.
5. Корисницима није дозвољено да врше измене на хардверу или инсталираном софтверу који је власништво Министарства правде без претходне писане дозволе.
6. У циљу заштите података служба за ИТ ће евидентирати коришћење мобилних уређаја у одговарајућим логовима, које ће у случају потребе користити за истраживања и утврђивања евентуалних злоупотреба.

Процедура се примењује на све стално запослене, запослене на одређено време или лица ангажована по другим основима, који имају приступ или користе мобилне уређаје у власништву Министарства правде.

Мобилни уређаји који се користе морају бити претходно одобрени и/или набављени од стране Министарства правде, и оцењени као компатибилни са захтевима обезбеђивања адекватног степена заштите.

Рад на даљину може се остварити и коришћењем уређаја који нису мобилни (на пример, десктоп рачунари). Ови уређаји, при томе, морају имати примењене најмање исте безбедносне мере као и сродни уређаји који се налазе у оквиру мреже, док се за заштиту комуникације морају применити исте мере као и за заштиту комуникације мобилних уређаја. Корисници ових уређаја морају обезбедити довољно безбедан простор за њихов рад (засебна соба, положај дисплеја такав да се онемогући посматрање од стране неовлашћених особа и слично).

Корисник мобилног уређаја у обавези је да сваки безбедносни инцидент пријави на емаил prijava.incidenta@mpravde.gov.rs без одлагања, а у року од 2 (два) сата од сазнања да се инцидент догодио да достави писану изјаву о околностима безбедносног инцидента. Под појмом безбедносни инцидент се сматра крађа, губитак мобилног уређаја или било који други догађај који доводи до нарушавања тајности и интегритета података који се налазе на мобилном уређају. Одговорно лице за ИТ (Менаџер безбедности информација) у СМФ-у је у обавези да, по пријави безбедносног инцидента, неодложно блокира несталом мобилном уређају приступ информационом систему и кориснику промени креденцијале за приступ. У случају да се пронађе мобилни уређај чији нестанак је пријављен, Одговорно лице за ИТ (Менаџер безбедности информација) у СМФ-у извршиће трајно брисање комплетног медијума за смештање оперативног система, апликација и података и поновну инсталацију оперативног система и потребних апликација. Под појмом „трајног брисања“ се сматра процедура брисања података на тај начин да се искључује могућност накнадног повраћаја тих података.

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

Члан 10.

Министарство правде 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. Њихове одговорности су утврђене уговором о раду или о ангажовању за рад ван радног односа и одговарајућим интерним актом.

Провера кандидата и услови запошљавања

Члан 11.

Министарство правде спроводи радње у циљу провере испуњености услова сваког појединачног кандидата за запослење, у складу са одговарајућим прописима и етичким правилима, сразмерно пословним захтевима, класификацији информација којима ће имати приступ и сагледаним ризицима.

Сви запослени и радно ангажовани појединци по другом основу којима је додељен приступ поверљивим информацијама, морају потписати **Споразум о поверљивости и неоткривању за физичка лица**, пре него што им се дозволи приступ опреми за обраду информација.

Обавезе у току запослења

Члан 12.

Руководство Министарства правде је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

Министарство правде у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

- Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;
- Штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама;
- Спроводи програме заштите на конзистентан и уједначен начин у свим организационим јединицама;
- Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

Запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења овог акта и процедура 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.

Упознавање са безбедношћу информација, стицање знања и обука

Члан 13.

Сви запослени као и одређени запослени у Министарству правде су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Дисциплински поступак

Члан 14.

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и у примени у Министарству правде.

Дисциплински поступак се покреће по предлогу Секретара Министарства правде или Менаџера безбедности информација.

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

Члан 15.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања. Дужности и обавезе које остају важеће и после престанка ангажовања и треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа, односно уговора о ангажовању лица ван радног односа.

Ова мера је ближе одређена:

- Уговором о раду
- Уговором о ангажовању лица ван радног односа
- Споразум о поверљивости и неоткривању за физичка лица.

За поступања приликом престанка запослења или ангажовања задужено је Одговорно лице за ИТ (Менаџер безбедности информација) у СМФу, који предузимају следеће активности:

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату,
- прегледа све налоге и приступе систему који су били доступни запосленом,
- преузима од запосленог електронске и друге мобилне уређаје,
- утврђује начин контакта са бившим запосленим након одласка,
- проверава враћене мобилне уређаје и уређаје за преношење података,
- даје налог за укидање налога електронске поште и свих других права приступа систему Министарства правде на дан престанка радног односа или другог основа ангажовања бившег запосленог,
- прегледа све налоге за приступ одлазећег запосленог и прикупља приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
- преузима картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми Министарства правде.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 16.

Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Пописивање имовине

Члан 17.

Одговорно лице за ИТ (Менаџер безбедности информација) у СМФу 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. Ово лице прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

У оквиру **Регистра информационе имовине** евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води Одговорно лице за ИТ (Менаџер безбедности информација) у СМФу.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај

Члан 18.

Појединци којима је дата одговорност за контролисање животног циклуса имовине дужни су да правилно управљају имовином током целог животног циклуса.

Министарство правде у оквиру **Процедуре за употребу ИКТ опреме и поступање са информацијама** уређује правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација. Запослени су дужни да потпишу **Изјаву о прихватљивом коришћењу информационе имовине**.

Запослени и екстерни корисници су обавезни да врате сву имовину Министарства правде коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

Током отказног рока запослених, Министарство правде контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности

Члан 19.

Класификовање података је поступак утврђивања и појединачног додељивања нивоа осетљивости податка, у складу са њиховим значајем за Министарство правде.

Министарство правде означава типове и локације података као осетљиве, пословне или јавне. Имовина се означава уз помоћ идентификационих налепница које носе одговарајућу класификациону ознаку.

Министарство правде класификациону шему поверљивости информација базира на три нивоа:

- откривање не изазива штету уопште или изазива мању непријатност или мању штету;
- откривање има значајан краткорочни утицај на пословање или тактичке циљеве;
- откривање има озбиљан утицај на дугорочне стратешке циљеве или угрожава опстанак.

Министарство правде врши класификацију ради:

- Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и постану 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.

Класификација документа мора да буде усклађена са правилима контроле приступа.

Министарство правде поступа у складу са усвојеним **Упутством за класификовање информационе имовине** и са датом матрицом коришћења класификованих информација. Посебним **Правилником за пренос опреме, медијума са информацијама изван просторија организације** заједно са **Налогом за пренос медијума са информацијама.** На овако уређен начин се дефинишу радње за поступање, обраду, складиштење и пренос података.

Поступање са имовином мора да подразумева:

- ограничења приступа која подржавају захтеве за заштиту сваког нивоа класификације;
- одржавање званичног записа о овлашћеним примаоцима имовине;
- заштиту привремених или трајних копија података на нивоу који је у складу са заштитом оригиналне информације;
- складиштење информационе имовине у складу са спецификацијама произвођача;
- јасно обележавање свих копија медија на које овлашћени прималац треба да обрати пажњу.

Заштита носача података

Члан 20.

Министарство правде обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, води СМФ, а информације са којима располаже Министарство, а које су настале у раду и у вези са радом Министарства, налазе се на носачима информација који се чувају:

- у архиви писарнице до истека текуће године, односно у архивском депоу;
- у Управи за заједничке послове републичких органа, Немањина 22-26;
- у електронској бази података Министарства, у Писарници;
- у Министарству, у Министарству финансија, Управи за трезор који се односе на финансијска документа о плаћању за потребе Министарства и на документацију везану за исплату плата запослених;
- у СМФу министарства - папирна документација која се односи на запослене у Министарству.

Управљање преносивим носачима података (медијума)

Члан 21.

Министарство правде је дужно да развија и имплементира процедуру о управљању преносним носачима, у складу са усвојеним **Упутством за класификовање информационе имовине.**

Директивом о коришћењу преносивих уређаја и бежичних веза, односно носача података садржи следеће одредбе:

- садржај сваког медијума који се може поново користити и који ће се износити изван организације, онда када више није потребан, треба да се неповратно избрише;
- за све медијуме који се износе из организације, онда када је то неопходно и изводљиво, треба захтевати одобрење, а о свим таквим изношењима треба водити евиденцију, како би се сачувао траг за проверу;
- све медијуме треба складиштити на безбедном и заштићеном месту, у складу са препорукама произвођача;
- коришћење криптографских техника за заштиту података на преносним медијумима, ако су поверљивост или интегритет података важни;
- подаци треба да буду пренети на нови медијум пре него што постану нечитљиви;
- вишеструке копије вредних података треба чувати на одвојеним медијумима да би се додатно смањио ризик од случајног оштећења или губитка података;
- да би се ограничила могућност губљења података, треба предвидети регистровање преносних медијума;
- покретне преносиве медијуме треба користити само ако за то постоји пословна потреба;
- уколико постоји пословна потреба за коришћењем преносивих медијума, неопходно је пратити пренос података на такве медијуме.

Расходовање носача података (медијума)

Члан 22.

Када више нису потребни, медијуми се расходују и уништавају на безбедан начин, применом **Оперативне процедуре информационе безбедности**.

Расходовање медијума на безбедан начин Министарство правде врши свођењем на минимум ризика од могућег преузимања осетљивих података од стране неовлашћених особа.

Безбедно расходовање медијума обухвата следеће активности:

- неопходно је уредити начин за идентификовање медијума који садрже осетљиве податке за које ће можда бити потребно безбедносно расходовање;
- медијуме који садрже осетљиве податке треба расходовати спаљивањем или кидањем, или брисањем података ради коришћења у неком другом апликативном програму унутар организације;
- расходовање медијума који садрже осетљиве податке је потребно евидентирати, како би се сачувао траг за проверу.

Физички пренос носача података (медијума)

Члан 23.

Носачи података који садрже информације се штите од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта. Када поверљива информација на медијуму није шифрована, потребно је додатно физички заштити медијум.

Смернице за безбедан транспорт дате су у **Директиви за пренос опреме, медијума са информацијама изван просторија организације**:

- користити поуздани транспорт или курире;
- потребно је увести проверу идентитета курира;

- карактеристике опреме за пренос морају да буду такве да обезбеде заштиту од свих физичких оштећења која би могла настати током преноса.

У случају транспорта носача података са информацијама, Секретар или друго овлашћено лице у Министарству одређује лице које ће вршити транспорт и начин транспорта.

Ограничење приступа подацима и средствима за обраду података

Члан 24.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном осетљивости података у складу са усвојеним **Упутством за класификовање информационе имовине** и са датом матрицом коришћења класификованих информација према члану 11. овог акта.

Процедура за контролу приступа заједно са **Табелом регистрације корисника** и **Табелом дерегистрације корисника** садржи попис свих информационих објеката и субјекте који им могу приступити.

Корисницима је дозвољен приступ само мрежи и мрежним услугама за чије коришћење су овлашћени.

Министарство правде ће посебним документом **Упутство за мрежну безбедност** уредити приступ мрежи и мрежним уређајима. Приступ мрежи и мрежним уређајима треба оперативно уредити тако да постоји:

- листа мрежа и мрежних услуга којима је приступ дозвољен;
- ауторизација ради утврђивања коме је одобрен приступ, којој мрежи и којим услугама;
- управљање заштитом приступа мрежним прикључцима и услугама;
- опис средстава која се користе за приступ мрежама и мрежним услугама;
- захтеви у погледу верификације корисника за приступ различитим мрежним услугама;
- надгледање коришћења мрежних услуга.

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

Члан 25.

Министарство правде управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

Управљање корисничким идентификаторима врши се уз поштовање следећих принципа:

- кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење;
- корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;
- периодично идентификовање и уклањање или онемогућавање вишеструких корисничких идентификатора;
- вишеструки идентификатори неког корисника се не издају другим корисницима.

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Додељивање привилегованих (администраторских) права на приступ врши се на основу одлуке одговорног лица.

Привилегована права на приступ додељују се посебно за сваки системски објекат уз дефинисан рок трајања тих права. Привилегована права на приступ која треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности. Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора. Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

Шифре за приступ општим корисничким идентификаторима администратора се мењају променом корисника.

Министарство правде једном годишње врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај запослења).

Запосленима, другим радно ангажованим и екстерним корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 26.

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

Сви корисници су дужни да:

- корисничко име и шифру држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
- избегавају чување корисничког имена и шифре у писаном облику;
- промене шифру када примете да постоји било какав наговештај могућег компромитовања.

Шифре морају да:

- Садрже најмање 9 алфанумеричких карактера;
- Садрже најмање једно велико и једно мало слово;
- Садрже најмање 1 број (0-9).

Шифре не заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и не смеју садржати више од 3 узастопна идентична бројчана или словна знака.

Корисници су дужни да привремене шифре промене приликом првог пријављивања.

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

Члан 27.

У циљу заштите података Министарство правде развија и имплементира политику коришћења криптографских контрола, и успоставља механизме и систем за управљање кључевима.

Криптозаштита обезбеђује:

- Аутентификацију (идентификацију корисника и других системских ентитета који захтевају приступ или одобрење акције корисника);
- Непорецивост (примена криптографских техника, најчешће дигиталног потписа, како би се добила потврда о извршавању или неизвршавању неке акције од стране појединачног корисника);
- Поверљивост (применом шифровања врши се заштита осетљивих или критичних информација које се складиште или преносе);
- Интегритет (непроменљивост података који се преносе).

Поступак криптографске контроле обухвата:

- анализу и процене потреба примене криптографије у пословним процесима укључујући опште принципе према којима би пословне информације требало да се штите;
- ниво заштите се одређује узимањем у обзир типа алгоритма за криптовање података, јачине и квалитета криптографског алгоритма;
- примену шифровања за заштиту осетљивих података приликом преноса мобилним или другим медијумима, уређајима или преко комуникационих водова;
- управљање кључевима (заштита криптографских кључева, повраћај шифрованих података у случају губљења, компромитовања или оштећења кључева).

Управљање кључевима

Члан 28.

Министарство правде примењује следеће методе за управљање кључевима које обухватају њихов цео животни циклус:

- генерисање кључева;
- издавање и добијање сертификата за јавне кључеве;
- складиштење кључева (кључеви се чувају на посебним уређајима или паметним картицама, на месту које је физички обезбеђено);
- дистрибуцију кључева (додела кључева намењеним ентитетима и активација самог кључа);
- замену или ажурирање кључева;
- поступак у случају компромитовања кључева;
- деактивацију кључева;
- обнављање изгубљених или оштећених кључева;
- прављење резервних копија или архивирање кључева;
- уништавање кључева;
- евидентирање и проверу активности у вези са управљањем кључевима.

Кључеви се могу користити само у периоду који одреди одговорно лице.

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

Члан 29.

Министарство правде је дужно да предузме мере ради спречавања неовлашћеног физичког приступа објекту, простору, просторијама и зонама у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација. Физичку заштиту објеката у којима је смештено Министарство правде врше припадници **Министарства унутрашњих послова**.

Зона раздвајања и успостављање система физичке безбедности

Члан 30.

Опрема за обраду информација се штити закључавањем просторија у којима се налази. У складу са проценом ризика дефинисане су следеће зоне раздвајања:

- у згради на локацији Немањина 22-26 која садржи опрему за обраду информација спољни кров, зидови и подови на тој локацији су од чврстог материјала, а сва спољна врата су потпуно заштићена од неовлашћеног приступа помоћу контролних механизама (решеткама, алармима, бравама итд.); врата и прозори су закључани у свим случајевима када су без надзора;
- постоје пријавнице са особљем МУП-а или друга средства за контролу физичког приступа до локације или зграде тако да је приступ локацијама или зградама ограничен само на овлашћено особље;
- сва пожарна врата у безбедносној зони раздвајања имају алармни уређај, под надзором су домаћина објекта УЗЗПРО и функционишу у складу са локалним противпожарним правилима у погледу осигурања од отказа;
- надгледање свих спољних врата и доступних прозора су под надзором домаћина зграде УЗЗПРО и МУП-а који обезбеђују и друге области, нпр. просторије са рачунарима или просторије за комуникације итд.;
- опрема за обраду информација којом управља Министарство физички је одвојена од оне којом управљају трећа лица.

Контрола физичког уласка

Члан 31.

Безбедносне области на локацији Немањина 22-26 су заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ, складу са смерницама МУП-а.

Смернице за контролу физичког уласка које се поштују:

- евиднетирање датума и времена уласка и изласка посетилаца уз надгледање, осим ако њихов приступ није претходно одобрен; приступ треба одобравати само за специфичне,

ауторизоване сврхе и издавати упутства о захтевима за безбедност области и о процедурама за ванредне ситуације;

- приступ областима у којима се обрађују или чувају поверљиве информације ограничен је само на овлашћене особе, применом одговарајућих контрола приступа, безбедно се одржава и надгледа евиденција свих приступа;
- од свих запослених, уговарача и треће стране, као и од свих посетилаца захтева се да носе видљиву идентификацију и да известе особље обезбеђења уколико наиђу на посетиоце без пратиоца или примете особу која не носи видљиву идентификацију;
- запосленима код пружаоца услуга обезбеђења (МУП) одобрен је ограничен приступ безбедносним областима или опреми за обраду осетљивих података и омогућен је када за то постоји потреба; овакав приступ треба да буде одобрен и надгледан у сваком тренутку;
- права приступа безбедносним областима редовно се преиспитују и ажурирају, а уколико постоји потреба и укидају.

Заштита канцеларија, просторија, средстава, као и заштита од претњи екстерних фактора из окружења

Члан 32.

Министарство правде обезбеђује и примењује одговарајућу контролу приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава. Такође, безбедним конфигурисањем се онемогућава приступ кључној опреми, а у циљу спречавања видљивости поверљивих информација, активностима споља. Физичка заштита се мора планирати и за случајеве природних катастрофа, непријатељских напада или несрећа.

Рад у безбедносним зонама

Члан 33.

Безбедносне зоне подлежу следећим мерама заштите:

- особље мора бити обавештено о активностима унутар безбедносне зоне;
- забрањује се рад без надзора у безбедносним зонама;
- безбедносне зоне које се не користе морају бити физички закључане и чија провера се врши периодично;
- не дозвољава се уношење фотографских, видео, аудио или других уређаја за записивање, осим уз претходно одобрење одговорног лица.

Евиденцију о уласку у безбедносну зону води Менаџер безбедности информација.

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

Члан 34.

Постављање и заштита опреме

Члан 35.

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа.

Смернице које се примењују за безбедност опреме јесу следеће:

- Опрема се поставља на месту које се може обезбедити од неовлашћеног приступа;
- Опрема за обраду информација која служи за приступ и коришћење осетљивих података се поставља не места која нису видљива неовлашћеним особама;
- Врши се редовна контрола система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, гас, електронске комуникације;
- Просторије са опремом треба редовно чистити од прашине;
- Забрањено је конзумирање хране и пића и пушење близини опреме за обраду информација;
- Редовно се прате температура и влажност ваздуха;
- Опрема мора бити заштићена од атмосферских падавина.

Менаџер безбедности информација редовно прати услове околине, као што су температура и влажност, који би могли негативно да утичу на рад опреме за обраду информација.

Помоћне функције за подршку

Члан 36.

Опрема се штити од прекида напајања, тако што се:

- помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
- капацитет помоћне опреме редовно процењује;
- редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова;
- обезбеђује вишеструко напајање са различитих траса.

Безбедносни елементи приликом постављања каблова

Члан 37.

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од прислушкивања, ометања или оштећења на следећи начин:

- водови напајања и телекомуникациони водови који улазе у просторије за обраду информација су подземни или имају адекватну алтернативну заштиту;
- каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње;
- за осетљиве или критичне системе се постављају оклопљени водови, користе се закључане просторије или кутије и примењује се електромагнетско оклапање ради заштите каблова;

- неовлашћено прикључење уређаја на каблове се врши техничким претраживањем и физичком провером;
- приступ до разводних табли и у просторије са кабловима се контролише.

Одржавање опреме

Члан 38.

Опрема се одржава како би се осигурали њена непрекидна расположивост и неповредивост, и то на следећи начин:

- опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;

  поправке и сервисирање опреме обавља само особље овлашћено за одржавање;
- о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;
- осетљиве информације се бришу из опреме;
- пре враћања опреме у рад након одржавања, потребно је прегледати како би проверили да није неовлашћено коришћена или оштећена.

Измештање и премештање имовине

Члан 39.

Опрема, информације или софтвер се измештају само уз одобрење одговорног лица, а током измештања се примењују следећа правила:

- треба да се одреде запослени и спољни корисници који имају овлашћење да одобре измештање имовине;
- треба да се поставе временска ограничења за измештање опреме и да се проверава усклађеност приликом повратка;
- треба документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања и ова документација треба да буде враћена са опремом, информацијама или софтвером.

Безбедност измештене опреме и имовине

Члан 40.

На измештену опрему треба применити безбедносне механизме заштите, узимајући у обзир различите ризике приликом рада изван просторија.

Безбедно расходовање или поновно
коришћење опреме

Члан 41.

Сви делови опреме који садрже медијуме за чување података потребно је верификовати да би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњени.

Безбедност опреме корисника без надзора

Члан 43.

Корисници треба да обезбеде да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.

Остављање осетљивих и поверљивих докумената и материјала

Члан 43.

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 (**правило чистог стола и екрана**).

Неопходно је да следеће активности буду примењене:

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. Носачи 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.
8. 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 44.

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, дефинишу се процедуре за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевивма измештања делова ИКТ система.

Усвајање и примена оперативних процедура

Члан 45.

Министарство правде успоставља документ **Оперативне процедуре информационе безбедности** које садрже инструкције за извршење следећих послова:

а) инсталација и конфигурација система;

б) обраду и поступање са информацијама (аутоматски и мануелно);

в) **Backup и Restore процедура** за израду резервних копија;

г) обрада захтева за временски распоред активности;

д) израда инструкција за поступање у случају грешке или у другим ванредним ситуацијама која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција;

е) израда инструкција за управљање осетљивим подацима у складу са **Упутством за класификовање информационе имовине**;

ж) **План опоравка ИТ услед катастрофе** за поновно покретање система и опоравак, које се користе у случају отказа система са листом контаката за подршку и ескалацију (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;

з) управљање системским записима (логовима);

и) процедуре за надгледање.

За усвајање, измене и допуне радних процедура овлашћен је Менаџер безбедности информација.

Управљање расположивим капацитетима

Члан 46.

Коришћење ресурса се, у складу са документом **Оперативне процедуре информационе безбедности** континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе система. Периодично се спроводе слеће активности:

а) брисање застарелих података;

б) повлачење из употребе апликација, система, база података или окружења;

в) оптимизација серије процеса и распореда;

г) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису критичне за пословање.

Раздвајање окружења за развој, испитивање и рад

Члан 47.

У складу са документом **Оперативне процедуре информационе безбедности,** окружења за развој, испитивање и рад су међусобно раздвојена, како би се смањио ризик од неовлашћеног приступа или промена у радном окружењу на начин да:

а) треба дефинисати и документовати правила за преношење софтвера из развојног статуса у оперативни статус;

б) развојни и оперативни софтвери треба да се извршавају на различитим системима или рачунарским процесорима, као и у различитим доменима или директоријумима;

в) промене у оперативним системима и апликацијама треба испитивати у окружењу за испитивање или режиму одржавања пре него што се примене на оперативне системе;

г) испитивање не треба да се ради на оперативним системима, осим у изузетним околностима;

д) компајлери, едитори и други развојни алати или системски помоћни програми не треба да буду доступни из оперативних система, ако се то не захтева;

ђ) да би се смањио ризик од грешке, корисници треба да примењују различите корисничке профиле за оперативне и системе за испитивање, а менији треба да приказују одговарајуће идентификационе поруке;

е) осетљиве податке не треба копирати у системско развојно окружење, осим ако нису обезбеђене еквивалентне контроле за систем за испитивање.

За обезбеђивање исправног и безбедног функционисања средстава за обраду података и примену радних процедура задужен је Менаџер безбедности информација.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 48.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен или неумрежен рачунар. У складу са **Упутством за управљање вирусима, DoS и Ransomware нападима**, 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.

Поступак контроле и предузимање мера против злонамерног софтвера

Члан 49.

Министарство правде одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

Суштина заштите од злонамерног софтвера своди се на:

1. формалну забрану коришћења неауторизованих софтвера;
2. имплементацију контрола које спречавају или откривају коришћење неовлашћеног софтвера;
3. имплементацију контрола које спречавају или откривају коришћење познатих или сумњивих компромитованих веб-сајтова;
4. успостављање формалног Упутства за управљање вирусима, DoS и Ransomware нападима ради заштите од ризика повезаних са добијањем датотека и софтвера од или преко спољних мрежа, или на било ком другом медијуму, указујући на то које заштитне мере треба предузети;
5. смањење рањивости које може да експлоатише непријатељски софтвер, нпр. кроз управљање техничким рањивостима у складу са **Процедуром управљања техничким рањивостима**;
6 спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе; присуство било каквих неодобрених датотека или неауторизованих допуна треба формално истражити;

7. инсталирање и редовно ажурирање софтвера за откривање злонамерног софтвера и опоравак ради претраживања рачунара и медијума као контролу из предострожности, или на рутинској основи.

У складу са **Упутством за управљање вирусима, DoS и Ransomware нападима**, листа провера које се спроводе:

а) проверу, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер;

б) проверу, пре коришћења, садржаја прилога електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер; ову проверу треба спроводити на разним местима, нпр. на серверима за електронску пошту, на стоним рачунарима или приликом уласка у мрежу оператора ИКТ система;

в) проверу постојања злонамерних софтвера на веб-страницама;

г) дефинисање процедура за менаџмент и одговорности за поступање са заштитом од злонамерног софтвера у системима, обука за њихово коришћење, извештавање и опоравак од напада злонамерним софтвером;

д) припрему одговарајућих планова за континуитет пословања приликом опоравка од напада злонамерним софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак;

ђ) имплементацију процедура за редовно прикупљање информација, као што је претплата на адресне спискове за доставу или провера веб-страница на којима се дају информације о новим злонамерним софтверима;

е) имплементацију процедура за верификовање информација о злонамерним софтверима и обезбеђење да су упозоравајући извештаји тачни и информативни; руководиоци треба да осигурају да се за разликовање лажних од стварних злонамерних софтвера користе квалификовани извори, нпр. проверени часописи, поуздане странице на Интернет мрежи или испоручиоци програма против злонамерних софтвера; сви корисници треба да буду свесни проблема појаве духовитих или злонамерних обмана и онога што треба да раде после њиховог пријема.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави Менаџеру безбедности информација или ИТ подршци.

У циљу заштите од упада у ИКТ систем, Менаџеру безбедности информација је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета Менаџеру безбедности информација може укинути приступ.

Заштита од губитка података

Члан 50.

Министарство правде, у складу са **Backup и Restore процедуром** за израду резервних копија заједно са записима **Backup план** и **Restore података,** врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација и података

Члан 51.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих и log фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Резервне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

За чување резервних копија користе се магнетне траке, екстерни хард дискови и CD/DVD медији.

Надлежна служба за ИТ подршку извршава следеће задатке:

- процењује осетљиве и критичне податке за које је потребно правити резервне копије;
- креира план прављења резервних копија;
- прави заштитне копије серверског оперативног система и података, комуникационог оперативног система и конфигурационих фајлова, апликација, сервиса и база података;
- верификује успешно прављење резервних копија;
- води евиденцију урађених резервних копија;
- одлаже копије на безбедно место;
- тестира исправност резервних копија и процедуре за прављење заштитних копија;
- рестаурира податке са резервних копија.

Backup план израде резервних копија информација обухвата следеће:

- тачне и потпуне записе о резервним копијама;
- обим и учесталост израде резервних копија;
- резервне копије треба да одражавају пословне потребе организације и критичност тих информација по континуитет пословања организације;
- треба их складиштити на локацији на довољној удаљености, како би се избегло свако оштећење на главној локацији;
- резервним копијама информација треба дати одговарајући ниво физичке заштите и заштите од утицаја околине (описано у тачки 12) који је доследан мерилима која се примењују на главној локацији;
- медијуме са резервним копијама треба редовно проверавати користећи запис **Restore података**, ради сигурности њихове употребе у ванредним ситуацијама и када је то неопходно;
- у ситуацијама у којима је важна поверљивост, резервне копије треба заштитити помоћу шифровања.

За заштиту од губитка података одговоран је Менаџер безбедности информација.

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

Члан 52.

У ИКТ систему Министарства правде формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу у складу са документом **Оперативне процедуре информационе безбедности**.

Записивање догађаја

Члан 53.

Министарство правде прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са информационом безбедношћу, који се морају чувати и редовно преиспитивати. Администратори система немају дозволу да бришу или деактивирају дневнике о сопственим активностима. Записи о догађајима садрже:

- идентификаторе корисника;
- активности система;
- датуме, време и детаље кључних догађаја, нпр. пријављивања и одјављивања;
- идентитет или локацију уређаја, ако је могуће, и идентификатор система;
- записе о успешним и одбијеним покушајима приступа систему;
- записе о успешним и одбијеним покушајима приступа подацима и другим ресурсима;
- промене у конфигурацији система;
- коришћење привилегија;
- коришћење системских помоћних функција и апликација;
- датотеке којима се приступало и врсте приступа;
- мрежне адресе и протоколе;
- аларме које је побудио систем за контролу приступа;
- активирање и деактивирање система заштите, као што су антивирусни системи и системи за откривање упада.

Заштита информација у записима

Члан 54.

Средства за записивање и записане информације су заштићени од неовлашћеног мењања и приступа.

Забрањено је неовлашћено уношење следећих измена:

- мењање типова порука које се записују;
- уношење измена у датотеке са записима или њихово брисање;
- препуњавање медијума за записе, што доводи до отказа записивања догађаја или уписивања преко већ раније записаног.

Записи администратора и оператора

Члан 55.

Активности администратора и оператора система се записују, а записи штите и редовно преиспитују. Власници привилегованих корисничких налога могу бити у стању да управљају записима на опреми за обраду информација која је под њиховом директном контролом, на који начин се штите и прегледају записи да би се одржала одговорност за привилеговане кориснике.

Сатови свих одговарајућих система за обраду информација заштите морају бити синхронизовани према UTC (eng. Coordinated Universal Time) времену, како би се обезбедила тачност свих логова, јер ће можда бити коришћени приликом истраге неког инцидента.

За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужен је Менаџер безбедности информација.

Обезбеђивање интегритета софтвера и оперативних система

Члан 56.

Министарство правде спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за управљање променама и инсталацију софтвера у оквиру документа **Оперативне процедуре информационе безбедности**.

Смернице за контролу промена и инсталацију софтвера своде се на то да:

- ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљени администратори, по добијању одговарајућег овлашћења од руководиоца;
- оперативни системи треба да садрже само одобрене извршне кодове, а не и развојне кодове или компајлере;
- апликације и оперативни системски софтвер треба имплементирати тек после обимног и успешно спроведеног испитивања, које обухвата испитивање применљивости, безбедности, утицаја на друге системе и погодности за коришћење, а треба их спроводити на засебним системима, односно тестним окружењима;
- треба осигурати да су све одговарајуће библиотеке изворних програма ажуриране;
- пре имплементације било каквих промена, треба успоставити стратегију повратка на претходно стање;
- приликом свих ажурирања на библиотекама оперативних програма, треба одржавати записе за проверу;
- као меру предострожности за неочекиване ситуације треба сачувати претходне верзије апликативног софтвера;
- старије верзије софтвера треба архивирати, заједно са свим потребним информацијама и параметрима, процедурама, детаљима конфигурације и софтвером за подршку, све док се подаци држе у архиви.

Инсталацију и подешавање софтвера може да врши само ИТ подршка, односно запослени корисник који има овлашћење за то.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 57.

Министарство правде врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

Управљање техничким рањивостима

Члан 58.

Министарство правде благовремено прикупља информације о техничким рањивостима информационих система који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимањем у обзир припадајућих ризика у складу са **Процедуром управљања техничким рањивостима**.

Посебне информације које су потребне за подршку управљања техничким рањивостима обухватају продавца софтвера, бројеве верзија, текуће стање размештаја, као и особе које су одговорне за тај софтвер.

Смернице за управљање техничким рањивостима своде се на то да:

- Министарство правде дефинише и успоставља улоге и одговорности у вези са управљањем техничким рањивостима, укључујући надзор, оцену ризика услед утврђене рањивости, исправке, следљивост имовине и све одговорности за потребна координирања;
- најмање једном месечно, а по потреби и чешће, врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др.) у циљу идентификације потенцијалних слабости ИКТ система.
- за софтверске и друге технологије (евидентиране у Регистру информацииоине имовине) се одређују информациони ресурси за идентификовање одговарајућих техничких рањивости и за одржавање свести о истима; ови информациони ресурси се ажурирају на основу измена у Регистру информационе имовине или онда када се идентификују нови или други корисни ресурси;
- дефинише се временски распоред реаговања на обавештење о могућим техничким рањивостима;
- када је могућа техничка рањивост идентификована, тада се идентификују припадајући ризици и акције које треба предузети; такве акције могу да обухвате исправке рањивих система и/или примену других контрола;
- у зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, предузете активности се спроводе у складу са контролама које су везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности у складу са **Процедуром за управљање безбедносним инцидентима**;
- ако је исправка доступна од легитимног извора, онда се оцењују ризици у вези са инсталирањем те исправке (ризике који настају услед рањивости треба упоредити са ризиком везаним за инсталирање исправке);
- исправке се морају прво испробати и вредновати пре него што се трајно угради, како би се осигурало да ће оне бити ефективне и да неће довести до споредних утицаја који се не могу толерисати; ако исправка није на располагању, онда треба размотрити друге контроле, као што су деактивирање услуга или могућности које се односе на рањивост,

прилагођавање или додавање контрола приступа, (нпр. заштитну баријеру на границама мреже) или појачано надгледање како би се открили или спречили постојећи напади и утицало на повећање свести о рањивости;

- о свим предузетим процедурама се праве записи за проверу, а процес управљања техничким рањивостима треба редовно надгледати и вредновати како би се осигурале његова ефективност и ефикасност;
- најпре се узимају у разматрање системи са високим ризиком;
- ефективан процес управљања техничким рањивостима се усклађује са активностима које се односе на управљање инцидентима, тако да обезбеди техничке процедуре које треба спровести ако се догоди неки инцидент;

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, Менаџер безбедности информација је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене рањивости. Прво се узимају у разматрање системи са високим ризиком.

Ограничења у погледу инсталације софтвера

Члан 59.

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедносним ризицима.

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

Члан 60.

Приликом спровођења ИТ ревизије ИКТ система, Министарство правде обезбеђује да ревизија има што мањи утицај на фукционисање система.

Поступак контроле информационих система:

- Са руководством су договорени захтеви за проверу приступа систему и подацима;
- Предмет и подручје испитивања за проверу су унапред договорени и строго контролисани;
- Испитивања за проверу су ограничена на приступ читањем;
- Приступ који није ограничен само на читање треба дозволити само за добијање издвојених копија системских датотека које се по завршеној провери бришу или се одговарајући штите уколико постоји обавеза да се такве датотеке чувају према захтевима за документовање провере;
- Захтеви за посебну или допунску обраду морају бити идентификовани и о томе мора бити сачињен писани споразум;
- Испитивања за проверу могу утицати на доступност система, па се покрећу ван радног времена;
- Сав приступ се надгледа и записује се да би се направио референтни траг провере.

Планирање и спровођење ИТ ревизије ИКТ система може да врши само Менаџер безбедности информација, односно други запослени или корисник који има овлашћење за то.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 61.

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

Спецификација мрежних услуга, било да се оне пружају унутар самог Министарства правде било од стране трећих лица, укључују механизме информационе безбедности и врсте услуга утврђених на захтев руководства. Мрежне услуге обухватају обезбеђивање прикључака, услуге на виртуалним приватним мрежама и мреже са додатним функцијама, као и решења за управљање безбедношћу (заштита и системи за откривање упада).

У мрежама су међусобно раздвојене групе информационих услуга, корисника и системи, а мрежни администратор је одговоран за управљање мрежом.

Менаџер безбедности информација је дужан/а да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Безбедност података који се преносе унутар Министарства правде, као и између Министарства правде и лица ван Министарства правде

Члан 62.

Заштита података који се преносе комуникационим средствима унутар Министарства правде, између Министарства правде и лица ван Министарства правде, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом следећих адекватних контрола:

- Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са успостављеним процедурама и адекватним контролама над спровођењем истих. Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

- Правила коришћења Интернета

Приступ садржајима на Интернету је дозвољен искључиво за пословне намене. На мрежи је омогућено надгледање, односно користи се поступак периодичне ревизије и контролисања логовања, како на пријему тако и на слању.

- Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намену коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

Споразуми о преносу информација

Члан 63.

Безбедан пренос пословних информација између организације и трећег лица обезбеђује се поштовањем споразума о преносу информација и спроводи се у складу са **Правилником за пренос опреме, медијума са информацијама изван просторија организације** коришћењем записа **Налог за пренос медијума са информацијама**.

Споразуми о преносу информација (у слободној форми прилагођени сваком конкретном случају) треба да укључе следеће:

1. одговорности руководства за контролу и извештавање о преносу, отпреми и пријему;
2. процедуре за обезбеђење следљивости и непорецивости;
3. минималне техничке стандарде за паковање и пренос;
4. стандарде за идентификовање курира;
5. обавезе и одговорности у случају инцидената нарушавања безбедности информација, као што је губитак података;
6. коришћење договореног система означавања осетљивих или критичних информација, уз осигуравање да је значење ознака одмах разумљиво и да су те информације заштићене на одговарајући начин;
7. посебне контроле које су потребне да би се заштитили осетљиви детаљи, попут криптографије;
8. одржавање ланца надзора за информације у току преноса.

Размена електронских порука

Члан 64.

Заштита информација укључених у размену електронских порука се регулише поштовањем правила безбедности у размени електронских порука.

Правила о поштовању безбедности у размени електронских порука обухватају:

- заштиту порука од неовлашћеног приступа, модификовања или одбијања услуга које су у складу са класификационом шемом датом у **Упутству за класификовање информационе имовине**;
- осигурање исправног адресирања и транспорта поруке;
- поштовање законских одредби, на пример захтеве за електронске потписе;
- добијање одобрења пре коришћења јавних спољних услуга, као што су размена хитних порука, приступ и коришћење друштвене мреже или заједничко коришћење датотека;
- строже нивое утврђивања веродостојности, контролисањем приступа из мрежа са јавним приступом.

Споразуми о поверљивости или неоткривању

Члан 65.

Споразум о поверљивости и неоткривању за правна лица као и **Споразум о поверљивости и неоткривању за физичка лица** имају за циљ заштиту информација Министарства правде и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

Да би се идентификовали захтеви за споразуме о поверљивости или неоткривању, треба узети у обзир следеће елементе:

1. дефиницију информација које треба заштитити;
2. очекивано трајање споразума, укључујући случајеве у којима је потребно да се поверљивост сачува неограничено;
3. поступања која се захтевају по истеку споразума, попут повраћаја или уништавања информација;

4. дозвољено коришћење поверљивих информација и пословних тајни, као и права потписника да користи информације;
5. право на проверу и праћење активности које укључују поверљиве информације;
6. процес за обавештавање и извештавање о неовлашћеном откривању или приступу поверљивим информацијама;
7. радње које треба предузети у случају кршења ових споразума.

Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 66.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, Министарство правде је у обавези да обезбеди информациону безбедност у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења. Менаџер безбедности информација је задужен за технички надзор над реализацијом од стране извођача, односно испоручиоца.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система Менаџер безбедности информација води документацију.

Документација из претходног става мора да садржи описе свих процедура, а посебно процедура које се односе на безбедност ИКТ система.

Анализа и спецификација захтева за информациону безбедност

Члан 67.

У захтеве за нове информационе системе или за побољшање постојећих информационих система морају бити укључени захтеви који се односе на информациону безбедност и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Захтеви за информациону безбедност укључују:

- Проверу идентитета корисника;
- Доступност, поверљивост, непорецивост и интегритет података и имовине;
- Надгледање пословних процеса;
- Омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке кориснике.

Спецификација захтева обухвата аутоматску контролу која ће бити уведена у информациони систем, као и потребу да постоји и ручна контрола, која мора бити примењена при вредновању развијених или купљених пакета софтвера, намењених за пословне апликације.

Системски захтеви за информациону безбедност и процеси за увођење безбедности се интегришу у фази дизајнирања информационих система.

Формално тестирање и процес имплементације ће се примењивати за све купљене производе.

У уговору са извођачем, односно испоручиоцем купљених производа, посебно се дефинишу захтеви за информациону безбедност.

У случају да безбедносна функционалност предложеног производа не задовољава одређен захтев, ризик и повезане контроле ће бити преиспитане пре куповине производа.

Обезбеђивање апликативних услуга у јавним мрежама

Члан 68.

Информације обухваћене апликативним услугама које пролазе кроз јавне мреже треба заштити од малверзација, неовлашћеног откривања података и модификовања. Неопхнодно је потврдити идентитет корисника и извршити поделу овлашћења и одговорности за постављање садржаја, електронског потписивања или обављања трансакција.

Заштита трансакција апликативних услуга

Члан 69.

Информације укључене у трансакције апликативних услуга се штите да би се спречио непотпун пренос, погрешно усмеравање, неовлашћено мењање порука, неовлашћено разоткривање, неовлашћено копирање порука или поновно емитовање.

Трансакције морају да подрже следеће услове:

- Обе стране које учествују у транскакцији морају да примене електронски потпис;
- Приватност свих страна које учествују у трансакцији;
- На комуникационим каналима примењено шифровање;
- Безбедност протокола који се користе у трансакцијама.

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

Члан 70.

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера наведених у овом члану.

За потребе испитивања и тестирања ИКТ система, односно делова система, Министарство правде избегава коришћење оперативних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачног добављача, купца, запосленог или др. Уколико се за сврху испитивања користе лични подаци или неке друге поверљиве информације, онда се сви осетљиви подаци и информације пре коришћења штите анонимизацијом личних података, уклањањем садржаја или изменом текста садржаја у предметном делу.

Уколико је за тестирање неопходно користити оперативне податке, примењују се следеће смернице:

- за свако копирање оперативних података у тестно окружење се издаје посебно овлашћење;
- приликом тестирања апликативних система примењују се процедуре за контролу приступа које се примењују и на оперативним системима;
- оперативне информације се одмах по завршетку испитивања бришу из тестног окружења.

За податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су подаци о личности коришћени приликом тестирања система, одговорно је Лице за

заштиту података о личности Министарства правде, у складу са Законом о заштити података о личности и другим прописима којима је дефинисана употреба и заштита такве врсте података.

За потребе тестирања ИКТ система, односно делова система, ИТ подршка, односно други запослени или корисник који има овлашћење за то може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

Приликом тестирања апликативних система примењују се додатне процедуре за контролу приступа путем физичке заштите и применом криптографских мера за заштиту система и података од неовлашћених приступа, а које се примењују и на оперативним системима. Скуп криптографских мера које ће бити примењене за заштиту података утврђује Менаџер безбедности информација, узимајући у обзир њихову поузданост исврсисходност.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 71.

Политика безбедности размене информација у пословним односима са пружаоцима услуга и између независних пружалаца услуга

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација Министарства правде морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

Пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са Министарством правде.

Министарство правде успоставља контролу безбедности информација која се односе на процесе и процедуре које ће спроводити пружаоци услуга за:

- идентификовање и документовање врсте пружаоца услуга којима ће Министарство правде дозволити приступ информацијама;
- стандардизовани процес за управљање односима између пружаоца услуга;
- дефинисање врста информација које ће различитим типовима пружаоца услуга бити дозвољено ради приступања, праћења и контроле приступа;
- минимални захтеви за безбедност информација за сваку врсту информација и врсту приступа;
- процеси и процедуре за праћење придржавања утврђених захтева за безбедност за сваку врсту добављача и врсту приступа;
- контроле за осигурање интегритета информација или обраде информација коју обезбеђује било која страна;
- поступање са инцидентима и непредвиђеним ситуацијама које су у вези са приступом пружаоца услуга, укључујући одговорности и организације и пружаоца услуга;
- управљање неопходним променама информација, опреме за обраду информација и свега осталог што треба да се премешта и осигурање да се безбедност информација одржава током прелазног периода.

Уговарање обавезе обезбеђивања безбедности у
споразумима са пружаоцима услуга

Члан 72.

Пре отпочињања преговора, потенцијални пружалац услуга у обавези је да потпише **Споразум о поверљивости и неоткривању за правна лица** или **Споразум о поверљивости и неоткривању за физичка лица**, која садржи обавезу за пружаоца услуга да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране Министарства правде , а за потребе извршења предмета преговора.

Потребно је да споразуми о поверљивости, односно уговор о пружању услуга, садржи одредбу о поверљивости са јасно утврђеном обавезом и одговорношћу пружаоца услуге уз претњу раскида уговора и накнаде штете у корист Министарства правде у случају повреде ове одредбе.

Пример: "Сви подаци и информације садржани у овом Уговору о пружању услуга се сматрају поверљивим пословним подацима и не смеју бити саопштени или на други начин учињени доступним трећим лицима. Нарочито се сматрају поверљивим сви пословни подаци и информације које једна страна учини доступним другој уговорној страни ради извршења обавеза из овог уговора, уколико ти подаци нису јавно доступни нити су били претходно познати другој страни.

Свака уговорна страна се обавезује да податке и информације које јој буду учињене доступним у складу са овим уговором и обавезом извршења уговорених послова и обавеза, буду стављене на располагање и увид запосленима, уколико је то неопходно ради извршења обавеза из овог уговора.

Уговорне стране се нарочито обавезују да поступају обазриво са подацима о личности до којих могу доћи у поступку извршења услуга за оператора ИКТ система, као и да те податке чувају и поступају у свему у складу са прописима који уређују заштиту података о личности.

У случају повреде ове обавезе уговорна страна чији су подаци коришћени има право раскида уговора и право да захтева накнаду штете услед неовлашћеног коришћења података и информација друге стране."

Пружаоци услуга дужни су да захтеве Министарства правде у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе.

Менаџер безбедности информација је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби правилника којима су такве активности дефинисане.

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

Члан 73.

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

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга са становишта информационе безбедности Менаџер безбедности информација редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

1. Надгледање и преиспитивање услуга се може вршити преко трећег лица;
2. Неопходно је да се поштују сви услови из споразума у вези са безбедношћу информација, као и да се спрече сви инциденти и проблеми нарушавања безбедности, те омогући управљање на одговарајући начин;
3. Врши се оцена квалитета извршења и саобразности уговорене услуге;
4. Пружалац услуге има уговорну обавезу да организује и припреми периодичне састанаке који ће обезбедити редовно извештавање Министарства правде и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;
5. Менаџер безбедности информација одржава потпуну контролу над спровођењем услуга и осигурава увид у све осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа страна приступа, које процесуира или којима управља;
6. Менаџер безбедности информација одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања;
7. Преиспитује трагове провере и записа о догађајима у вези са информационом безбедношћу код пружаоца услуга, односно оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене; утврдити поступак извештавања, праћења и поступања у складу са захтевима Министарства правде у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета пружаоца услуга.

Приликом надзора над извршењем квалитета и саобразности уговорене услуге проверава се да ли пружалац услуге задовољава све критеријуме који су били од пресудног значаја приликом избора, укључујући обим и квалитет услуге, као и да се у току поступка извршења услуге може утицати на побољшање квалитета услуге или начина и обима извршења, у складу са утврђеним стварним потребама Министарства правде.

У поступку објективне евалуације квалитета и обима пружене услуге у односу на уговорену, потребно је прикупити све релевантне чињенице, податке и документацију у вези са извршењем услуге, као и прикупити податке од непосредних, крајњих, корисника у вези са предметом услуге. Евалуација се може извршити слањем упитника, разговором са изабраним појединцима или на основу анонимног анкетирања путем електронске поште.

Управљање променама уговорених услуга од стране пружаоца услуга

Члан 74.

Уговором са пружаоцем услуга треба обезбедити могућност континуираног управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контролу безбедности информација.

Промене које се узимају у обзир су промене у споразумима са пружаоцима услуга, повећање обима текућих услуга које се нуде, као и промене које уводи Министарство правде ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

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

Члан 75.

Одговорност појединаца и поступак одговора на инциденте

Посебном **Процедуром за управљање безбедносним инцидентима** и записима **Пријава безбедносног инцидента**, **Извештај о реакцији на безбедносни инцидент** и **Процена утицаја безбедносног инцидента** се уређује начин одговора на инциденте нарушавања информационе безбедности и одређује особа овлашћена за контакт у случајевима нарушавања безбедности, као и контакт са надлежним органима.

Процедуром се одређују следеће неопходне активности у вези са инцидентом:

- припрема и планирање одговора на инциденте;
- надгледање, детекција, анализа и извештавање о догађајима и инцидентима у вези са безбедношћу информација;
- записивање активности у оквиру управљања инцидентима;
- поступање са судским доказима;
- оцењивање и одлучивање о догађајима у оквиру безбедности информација и оцењивање слабости у погледу безбедности информација;
- одговарање на инциденте, опоравак од инцидента и комуникацију са екстерним или интерним особама или организацијама.

Министарство правде одређује да је Менаџер безбедности информација, чији је задатак да придржавајући се процедура одређених овим чланом, планира, детектује, анализира и информише надлежне у току и након инцидента.

За Менаџера безбедности информација се подразумева да поседује одговарајућа техничка знања како би на најбржи и одговарајућу начин могао/гла да одговори на безбедносне инциденте.

Менаџер безбедности информација у циљу превенције од безбедносних ризика обезбеђује више (различитих и другачијих) мехнизама за комуникацију и координацију у случају нарушавања безбедности. Ови механизми могу бити бити: обезбеђивање контакт информација (број телефона, електронска адреса) појединаца и чланова тима у оквиру организације и ван ње, систем за праћење проблема (тикет систем), шифровани софтвер који би био коришћен од стране појединаца у оквиру организације и спољашних странака, посебну осигурану просторију за чување података и складиштење поверљивог материјала итд.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени или корисник је дужан да о томе одмах обавести Менаџера безбедности информација.

Извештавање о догађајима у вези са безбедношћу информација

Члан 76.

Сви запослени морају бити упознати са обавезом и процедуром извештавања о догађајима у вези са информационом безбедношћу.

Менаџер безбедности информација је дужан да припреми план и неколико метода комуникације које би могле да се примене у зависности од инцидента. Могуће методе комуникације су: електорнска пошта, веб сајтови (интерни, екстерни, портали), телефонска комуникација, говорна порука, писмено извештавање, директан контакт.

У случају погрешног функционисања или других аномалијских понашања система врши се исто извештавање као и у случају догађаја у вези са информационом безбедношћу на следећи начин:

1. Запослени који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и послати га електронском поштом Менаџеру безбедности информација на prijava.incidenta@mpravde.gov.rs као и позвати телефоном или пријавити проблем путем Интернет стране за help desk;
2. Адресу електронске поште и Интернет страну за help desk проверава Менаџер безбедности информација;
3. Менаџер безбедности информација врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури.

Када је индетификован инцидент запослени је дужан да одмах обавести Менаџера безбедности информација, и предузме мере у циљу заштите ресурса ИКТ система.

Менаџер безбедности информација води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са Уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Извештавање о утврђеним слабостима система заштите

Члан 77.

Сви запослени су у обавези да о уоченим и утврђеним слабостима ИКТ система известе Менаџера безбедности информација, у што краћем року, како би се инциденти нарушавања информационе безбедности спречили и спречио настанак штете. Одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему, који могу да имају значајан утицај на нарушавање информационе безбедности, поступа у складу са одговарајућом процедуром.

Догађаји у вези са информационом безбедношћу се оцењују и у складу са анализом се доноси одлука да ли је потребно да се класификују као инциденти нарушавања информационе безбедности.

Одговор на инциденте нарушавања информационе безбедноости

Члан 78.

Министарство правде је утврдило **Процедуру за управљање безбедносним инцидентима** којом се дефинишу одговорна лица задужена за превенцију и реаговање, план поступања у случају опасности од настанка безбедносних инцидената или настанка безбедносних

инцидената, обавезу вођења евиденције о предузетим активностима, обавезуизвештавања и размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама.

Министарство правде овим актом обавезује све запослене и пружаоце услуга да Менаџеру безбедности информација без одлагања пријављују безбедносне слабости, претње и инциденте у ИКТ систему.

Министарство правде је у обавези да одреди одговорно лице/а у СМФу за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности.

Прикупљање доказа

Члан 79.

Министарство правде дефинише и примењује **Процедуру за управљање безбедносним инцидентима** која обезбеђује процесе за идентификацију, прикупљање и чување информација које могу да послуже као доказ ради покретања дисциплинског, прекршајног или кривичног поступка. Прикупљено знање из анализе и решавања инцидената који су нарушили информациону безбедност, Министарство правде користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

Мере које обезбеђују континуитет обављања
посла у ванредним околностима

Члан 80.

Министарство правде према **Плану опоравка ИТ услед катастрофе (IT Disaster Recovery Plan)** примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

Планирање континуитета мера безбедности информација

Члан 81.

Континуитет пословања се осигурава кроз План опоравка ИТ услед катастрофе уз који се такође чува:

- документација са логичким и физичким дијаграмима ИКТ система и копије пројеката;
- заштитне копије конфигурационих фајлова и оперативног система активних уређаја;
- евиденција о евентуалном постојању резервне опреме;
- унапред направљене конфигурације за различите сценарије;
- резервне копије података.

План опоравка ИТ услед катастрофе је документ који је подложан сталним изменама, па је неопходно у континуитету вршити:

- процену најкритичнијих апликација, података, конфигурационих фајлова и системског софтвера за који треба направити резервне копије;
- одређивање места чувања резервних копија;

- одређивање нове локације рада ИКТ система у случају немогућности рада на основној локацији/избор рачунара који ће привремено заменити сервер док се сервер не стави у функцију;
- ажурирање података о тиму који ће бити ангажован на отклањању последица нежељених догађаја;
- одређивање извора непрекидног напајања електричном енергијом;
- проверу постојања документације за сервисе, апликације и базе података;
- проверу процедуре инсталације и конфигурисања сервиса, апликација и база података;
- проверу места чувања апликација и база података и резервних копија података.

Имплементација континуитета безбедности информација

Члан 82.

Да би се осигурао потребан ниво континуитета безбедности информација током ванредних ситуација, Менаџер безбедности информација примењује процедуре и контроле описане у **Плану опоравка ИТ услед катастрофе (IT Disaster Recovery Plan)**.

Менаџер безбедности информација редовно врши проверу усвојених процедура контроле континуитета безбедности информација, како би оне биле адекватне и ефективне током ванредних ситуација.

Провера се врши вежбањем и испитивањем знања и рутине приликом руковања процесима, процедурама и контролама, као и преиспитивањем ефективности мера безбедности информација у случају промене информационих система, процеса, процедуре и контроле безбедности информација.

III. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Министарства правде

Члан 83.

Обавеза Министарства правде је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Акта о безбедности ИКТ система, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Министарства правде.

Ступање на снагу и објављивање

Члан 84.

Овај Акт о безбедности информационо-комуникационог система Министарства правде ступа на снагу даном објављивања на огласној табли и интернет страни Министарства правде.

У Београду, 27. децембар 2023. године
Број: 030-03-00048/2023-34

М И Н И С Т А Р
Маја Поповић