На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/16), 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) и члана 15. став 1. тачка 13) Статута Директората за радијациону и нуклеарну сигурност и безбедност Србије, Одбор Директората је на IV седници одржаној дана 08. септембра 2023. године, донео

ПРАВИЛНИК

о безбедности информационо-комуникационог система Директората за радијациону и нуклеарну сигурност и безбедност Србије

I. ОСНОВНЕ ОДРЕДБЕ

Предмет Правилника
Члан 1.

Овим Правилником ~~се~~ ближе се уређују мере заштите информационо-комуникационог система, нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система (у даљем тексту: ИКТ систем), као и овлашћења, дужности и одговорности корисника информатичких ресурса Директората за радијациону и нуклеарну сигурност и безбедност Србије (у даљем тексту: Директорат).

Значење појединих термина
Члан 2.

Изрази употребљени у овом Правилнику имају следеће значење:

1) информационо-комуникациони систем (ИКТ систем) је технолошко - организациона целина која обухвата:
   1. електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
   2. уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
   3. податке који се, обрађују, претражују или преносе помоћу средстава из електронске комуникационе мреже и воде, чувају уређаји или групе међусобно повезаних уређаја, а у сврху њиховог рада, употребе, заштите или одржавања;
   4. организациону структуру путем које се управља ИКТ системом;
   5. све типове системског и апликативног софтвера и софтверске развојне алате.
2) информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;
3) тајност је својство које значи да податак није доступан неовлашћеним лицима;
4) интегритет значи очуваност изворног садржаја и комплетности податка;
5) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
6) аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

7) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
8) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
9) управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;
10) инцидент је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система;
11) мере заштите ИКТ система означавају скупно све мере информационе безбедности које се примењује у оквиру Директората, а тичу се коришћења ИКТ система, превенције безбедносних инцидената, умањења ризика од безбедносних инцидената, као и реакције у случају наступања безбедносног инцидента, едукације и других мера у циљу обезбеђивања висиоког нивоа информационе безбедности у оквиру Директората. Мерама заштите се обезбеђује превенција од настанка инцидената и минимизација штете од инцидента који угрожавају обављање делатности Директората. Овим мерама се врши заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и деструкције, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани;
12) крипто-заштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
13) информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура, унутрашње опште акте, процедуре и слично;
14) Треће лице је правно или физичко лице са којим Директорат сарађује по основу уговора о одржавању или имплементацији ИКТ система или његових делова;
15) Корисник је запослени Директората који има приступ ИКТ систему ради обављања пословних активности;
16) Сарадник за ИТ је запослени коме је дозвољена администрација ИКТ система;
17) креденцијал је идентификатор (корисничко име и лозинка; картица; ПИН код; 1Р адреса и сл.) на основу кога се врши аутентикација и ауторизација приступа ИКТ систему;
18) кориснички налог чине креденцијали Корисника помоћу кога је Кориснику омогућен обим приступа ИКТ систему, у складу са пословима које обавља у Директорату;
19) администраторски налог чине креденцијали Администратора (Сарадника за ИТ) помоћу кога се омогућава администрирање ИКТ система или његових делова.
20) VPN (*Virtual Private Network* - Виртуелна приватна мрежа) је сигурна криптована интернет веза која физички удаљеном рачунару омогућава приступ мрежи Директората као и ресурсима ИКТ система.

Циљеви Правилника о безбедности
Члан 3.

Циљеви на којима се заснива овај Правилник се односе на:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности ИКТ система;
2. спречавање и ублажавање последица безбедносних 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 Правилника о безбедности
Члан 4.

Сва запослена и на други начин радно ангажована лица (у даљем тексту: запослени) дужна су да примењују мере заштите ИКТ система које су ближе уређене овим Правилником и које служе превенцији од настанка и минимизацији штете од инцидената. Мере заштите се примењују у свим организационим нивоима и на свим радним местима.

Запослени у Директорату морају бити упознати са садржином овог Правилника и дужни су да поступају у складу са њим, као и другим интерним процедурама којима се регулише информациона безбедност.

Директор, као законски заступник Директората, одговоран је за праћење и примену мера заштите ИКТ система у оквиру институције.

Помоћници директора одговорни су за праћење и примену мера заштите ИКТ система у оквиру сектора којима руководе, и од стране запослених у оквиру тих сектора.

Одговорност запослених
Члан 5.

Запослени су дужни да приступају информацијама и ресурсима ИКТ система искључиво ради обављања редовних пословних активности.

Запослени су дужни да све безбедносне инциденте или проблеме пријаве сараднику за развој и одржавање информационог система (у даљем тексту: сарадник за ИТ).

Сарадник за ИТ, без одлагања обавештава директора или помоћнике директора о инцидентима из става 2 овог члана Правилника, у зависности од тога да ли безбедносни инцидент погађа целу институцију или њен поједини организациони део и предлаже мере заштите ИКТ система.

Непоштовање одредби овог Правилника, као и свако угрожавање или нарушавање информационе безбедности, представља повреду радне обавезе и повлачи дисциплинску одговорност запосленог, у складу са општим прописима о раду, Правилником о раду Директората и другим интерним актима Директората.

Предмет заштите
Члан 6.

Мере заштите ИКТ система односе се на:
- електронске комуникационе мреже;
- електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма;
- оперативне и апликативне рачунарске програме;
- програмски код;

- податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја;
- организациону структуру путем које се управља ИКТ системом;
- корисничке налоге;
- информације за проверу веродостојности;
- техничку и корисничку документацију;
- унутрашње опште акте и процедуре.

II. МЕРЕ ЗАШТИТЕ

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру Директората
Члан 7.

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

Овим Правилником, другим општим актима, појединачним актима и процедурама Директората уређују се обавезе и одговорности запослених, правних и физичких лица у вези са управљањем информационом безбедношћу.

Приликом ступања на рад сваки новозапослени се од стране Сарадника за ИТ упознаје са Правилником и прописаним мерама заштите и потписује изјаву којом потврђује да је прочитао, разумео и прихватио обавезе у области примене и праћења мера заштите ИКТ система.

Приступ ИКТ систему је условљен радним задужењима и обавезама које свако од запослених има у опису свог радног места, а подразумева да запослени приступа само оним деловима система који су неопходни за обављање његових радних задатака (тзв. *need to know*), с циљем да се смањи ризик од злоупотреба, неовлашћених приступа, нарушавања интегритета података у ИКТ систему и људске грешке.

Процедуром о правима приступа ИКТ систему, Директорат утврђује начин доделе овлашћења за приступ ИКТ систему, начин измене и укидања права приступа у случају када дође до промене радног статуса запосленог – корисника као и поступак заштите ИКТ система у случају губитка или крађе креденцијала (односно параметара за приступ, попут корисничког имена или лозинке).

Уговором о раду и другим општим актима утврђује се и прописују обавезе и одговорности сваког запосленог и одговорног лица, у случају непоштовања одредби које уређују информациону безбедност.

Постизање безбедности рада на даљину и употребе мобилних уређаја
Члан 8.

Радни однос и обављање послова ван просторија послодавца обухвата: рад на даљину, рад од куће и виртуелно радно окружење. Такође, рад на даљину у смислу овог Правилника односи се на ситуацију када је запослени дужан да изврши одређене послове на мрежи Директората, а налази се ван просторија Директората.

Правила и услови за повезивање на мрежу Директората са удаљене локације дефинисана су Процедуром за *VPN* приступ информационом систему.

Процедура за *VPN* приступ информационом систему се примењује на запослене који обављају рад на даљину на радним станицама које су у власништву Директората, укључујући и трећа лица са којима се *VPN* приступ дефинише уговором.

Директорат дозвољава рад на даљину и употребу мобилних уређаја од стране запослених, уколико је то потребно за обављање радних задатака и 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.

Коришћење мобилних уређаја
Мобилни уређаји подразумевају све преносне електронске уређаје намењене за комуникацију на даљину. У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони, *PDA*, као и сви други мобилни (преносни) уређаји који садрже податке и имају могућност повезивања на мрежу.

Коришћење мобилних уређаја као и повезивање на мрежу Директората путем мобилних уређаја дефинисани су Процедуром о коришћењу мобилних уређаја.

Процедура о коришћењу мобилних уређаја се примењује на све запослене који имају приступ или користе мобилне уређаје у власништву Директората укључујући и трећа лица са којима се употреба мобилних уређаја дефинише уговором.

За мобилне уређаје важе све мере заштите које се примењују за уређаје у оквиру централног ИКТ система, а подешавање мобилних уређаја спроводи сарадник за ИТ.

Сарадник за ИТ је одговоран за вођење евиденције о свим мобилним уређајима у власништву Директората.

Оспособљеност за коришћење ИКТ система
Члан 9.

Директорат се стара да запослени који управљају ИКТ системом као и запослени који користе ИКТ систем имају адекватан степен образовања и способности као и свест о значају послова које обављају.

Директорат 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.

Дужност чувања поверљивости информација
Члан 9а.

Запослени којима је додељено право приступа поверљивим информацијама, као и информацијама које су од значаја за ИКТ безбедност, пре ступања на рад, односно пре него што им се дозволи приступ опреми за обраду информација дужни су да потпишу уговор о поверљивости (*NDA - Non-Disclosure Agreement* или други слични уговор), изјаву о поверљивости или други документ којим гарантују да ће поштовати дужност чувања поверљивости информација у складу са овим чланом.

Запослени су дужни да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система Директората, и након престанка или промене радног ангажовања. Ближе мере за очување поверљивости прописане су Процедуром о правима приступа ИКТ систему, уговорима и изјавом о поверљивости.

Едукација из области заштите информационе безбедности
Члан 9б.

Запослени су обавезни да путем едукације редовно стичу нова и обнављају постојећа знања о безбедносним ризицима који могу угрозити ИКТ систем.

Запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура континуирано се обучавају у циљу унапређења техничког и технолошког знања.

Директор, кабинет директора и сарадник за ИТ су ауторизовани за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Сви запослени 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.

Директорат се стара да сарадник за ИТ који администрира поверљиве, пословне и интерне податке, периодично похађа екстерну едукацију из области безбедности ИКТ система.

Сарадник за ИТ
Члан 9ц.

Сарадник за ИТ је запослени у Директорату коме је дозвољена администрација ИКТ система. Сарадник за ИТ је овлашћен за:

1. интерну појединачну или групну едукацију запослених из области ИКТ безбедности;
2. праћење, анализу, извештавање и предузимање активности на плану спровођења мера заштите и процедура ИКТ безбедности;
3. предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите;
4. спровођење активности у односу на попис информационих добара, хардверских и софтверских компоненти, и других компоненти релевантних за област информационе безбедности, у складу са одредбама овог Правилника;
5. друге активности прописане одредбама овог Правилника.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених у Директорату
Члан 10.

Након престанка радног ангажовања, Кориснику се укида право приступа ИКТ систему Директората у складу са Процедуром о правима приступа ИКТ систему.

Корисник је дужан да чува поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система током радног ангажовања као и након престанка или промене радног ангажовања, што се уређује уговорима и изјавом о поверљивости.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту
Члан 11.

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

Пописивање Информационих добара
Члан 11а.

Пописна комисија Директората једном годишње, у складу са примењивим прописима, врши попис имовине, у оквиру чега се води и евиденција хардверских и софтверских компоненти.

Попис Информационих добара, хардверских и софтверских компоненти, као и других компоненти релевантних за област информационе безбедности, врши се у сарадњи са сарадником за ИТ.

Сарадник за ИТ води евиденцију информационих добара која одражава реално стање ИКТ система и у којој се евидентирају:

- сва информациона добра, опрема и софтвери који се користе за израду, обраду, чување, пренос, брисање и уношење података у оквиру ИКТ система;
- запослени који су одговорни за заштиту за свако информационо добро, опрему и софтвере;
- друге информације релевантне за стање ИКТ система.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај
Члан 11б

Запослени у Директорату дужни су да правилно управљају ИКТ имовином којом су задужени током целог животног циклуса те имовине.

Директорат у оквиру интерног акта о руковању имовином уређује, између осталог и правила за прихватљиво коришћење информационих добара.

Запослени и трећа лица су обавезни да врате сву имовину у власништву Директората коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

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

Класификовање података тако да ннво њнхове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информациопој безбедности
Члан 12.

Класификовање податка је поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу са њиховим значајем за Директорат.

Ниво заштите података у оквиру ИКТ система Директората мора да:

- одговара осетљивости и важности података;
- одговара штети која може настати услед неовлашћеног откривања, измене, брисања или уништења података;
- је у складу је са примењивим прописима који уређују питања заштите података као што су пословна тајна, тајни подаци и подаци о личности.

Класификациона шема поверљивости података Директората базира се на следећа четири нивоа поверљивости података:

- **Поверљиви подаци** обухватају све поверљиве и власничке информације у вези са производима, услугама, пословањем (укључујући финансијске, техничке и друге аспекте и карактеристике пословања), опремом, материјалном и нематеријалном имовином и уопште ресурсима Директората које нису опште познате јавности, укључујући, а не ограничавајући се на софтвер (нпр. извор, објекат и извршни код у штампаној форми и електронском формату) и хардвер који се односе на имплементацију било које технологије даваоца информација; све пословне, кадровске податке, податке о запосленима, клијентима, техничке, комерцијалне или финансијске информације. Поверљиве информације обухватају документе, цртеже, извештаје, корисничке и администраторске креденцијале и друге записе на свим носачима и обавештења који садрже, позивају се или се заснивају на било којим „Поверљивим информацијама".

- **Пословни подаци** су сви подаци на које се односи Закон о заштити пословне тајне ("Службени гласник РС", број 72/11) и Правилник о заштити пословне тајне Директората.

- **Интерни подаци** су сви подаци из документације Директората, као и подаци о запосленима и предметима /документацији клијената на које се односи Закон о заштити података о личности ("Службени гласник РС", бр. 97/08, 104/09 - др. закон, 68/12 - одлука УС и 107/12).

- **Јавни подаци** представљају оне информације које су јавно доступне и чије откривање не изазива никакву штету. То су подаци који су доступни на сајту Директората, на друштвеним мрежама, као и подаци који се јавно презентују.

Приступ поверљивим подацима имају само запослени који због природе свог посла морају да буду упознати са таквим подацима (*Need to know* принцип). Поверљиви подаци не смеју да се складиште ван ИКТ система Директората.

Приступ подацима о личности уређује се овим Правилником и документима Директората који уређују заштиту података о личности.

Право и обим приступа пословним и/или интерним подацима остварују запослени путем својих креденцијала, који се додељује, мењају или укидају у складу са Процедуром о правима приступа ИКТ систему. Руковање пословним и интерним подацима ИКТ система се спроводи у складу Процедуром за поступање, обраду, складиштење и пренос података.
Приступ јавним подацима имају сва заинтересована лица, у складу са посебним законима.

Заштита носача података
Члан 13.

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

Носач података је уређај или медијум који служи за складиштење и пренос података на физичком или виртуелном нивоу. Овај сегмент опреме обухвата дискове који су фиксни део ИКТ система, али и уређаје и носаче који се користе за пренос података (УСБ меморије, екстерни дискови, ЦД, ДВД, као и остали предмети и компоненте који имају могућност чувања и преноса података).
Евиденцију носача на којима су снимљени подаци, води сарадник за ИТ.

Употреба носача података
Члан 13а.

У оквиру ИКТ система Директората дозвољено је коришћење свих носача података који су власништво Директората и који се користе на следећи начин:

- Дискови сервера, као носачи поверљивих, пословних и интерних података се користе искључиво у просторијама Директората и за њихову безбедност задужен је сарадник за ИТ.
- Дискови рачунара, као носачи пословних и интерних података, се користе искључиво у просторијама Директората и за њихову безбедност су задужени запослени који користе радне станице за обављање пословних активности.
- Дискови мобилних рачунара или екстерна меморија осталих мобилних уређаја, као носачи пословних и интерних података, се може користити на безбедном месту које је и ван просторија Директората. За њихову безбедност су задужени запослени који користе и дуже мобилни уређај или екстерну меморију за обављање пословних активности.

Употреба носача података на којима су пословни, интерни или јавни подаци прописана је Процедуром за поступање, обраду, складиштење и пренос података.

Носачи података који су фиксни део ИКТ система (дискови сервера и радних станица) не могу да се користе у другим ИКТ системима док се подаци који су записани на њима трајно не униште.

Управљање преносним носачима података (медијума)
Члан 13б.

Запослени који користе преносне носаче података за пренос пословних, интерних или јавних података у пословне сврхе, дужни су да поступају у складу са Процедуром за управљање преносним носачима података и задужени су за њихову безбедност.

Расходовање носача података (медијума)
Члан 13в.

По престанку потребе за њиховим коришћењем, носачи података се расходују на безбедан начин, применом Процедуре за безбедно расходовање носача података.

Расходовање носача података на безбедан начин Директорат врши свођењем на минимум ризика од могућег преузимања осетљивих података од стране неовлашћених особа.

Физички пренос носача података
Члан 13г.

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

Мобилни уређаји се транспортују у складу са Процедуром о коришћењу мобилних уређаја.

Преносни носачи података се транспортују у складу са Процедуром за управљање преносним носачима података.

У случају транспорта носача података са информацијама, сарадник за ИТ ће организовати транспорт на прикладан и безбедан начин, у складу са смерницама за безбедан транспорт.

Ограничење приступа подацима и средствима за обраду података
Члан 14.

Приступ подацима у ИКТ систему Директората је дозвољен само лицима која за то имају правни основ.

Приступ поверљивим подацима ИКТ система Директората имају само одговарајући запослени који су истовремено и одговорни за њихову безбедност.
Приступ пословним и интерним подацима ИКТ система Директората је ограничен тако да је кориснику ИКТ система омогућен приступ само оним подацима и деловима ИКТ система који су му потребни за реализацију радних активности (*Need to Know* принцип). Сваком кориснику се додељује, мења или укида право приступа пословним и интерним подацима у складу са Процедуром о правима приступа ИКТ систему и Процедуром о приступу мрежи и мрежним уређајима.
Приступ јавним подацима имају сви запослени.

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему н услугама које ИКТ систем пружа
Члан 15.

Одобравање овлашћеног и спречавање неовлашћеног приступа ИКТ систему Директората врши се:

- хардверски, где се приступ додељује, мења и укида у складу са Процедуром о приступу мрежи и мрежним уређајима
- корисничким креденцијалима.

Кориснички креденцијали се састоје од корисничког имена и лозинке, где се лозинке сматрају поверљивим подацима. Кориснички креденцијали могу имати форму администраторског или корисничког налога који се додељују, евидентирају, мењају или укидају у складу са Процедуром о правима приступа ИКТ систему.

Овлашћен приступ ИКТ систему Директората је одобрен само лицима са администраторским или корисничким налогом.

Додела и коришћење администраторских налога је контролисана и ограничена само на администратора система - сарадника за ИТ, или трећа лица у складу са уговором. Додела и коришћење корисничких налога је контролисана и ограничена само на запослене у

Директорату који користе ИКТ систем за обављање радних задатака.

Запосленима и трећим лицима укида се право на приступ ИКТ систему по престанку радног односа у Директорату или по истеку уговора.

Утврђивање одговорности Корисника за заштиту сопствених средстава за аутентикацију
Члан 16.

Приступ ИКТ систему Директората базиран је на корисничким креденцијалима и корисници ИКТ система су дужни да поштују следећа правила:

1 сарадник за ИТ креира корисничке креденцијале са привременом лозинком за приступ. Приликом првог приступа систему корисник креира сопствену шифру за приступ у складу са Процедуром о правима приступа ИКТ систему.
2 све лозинке корисника се чувају у базама или датотекама ИКТ система које се налазе на серверима, у енкриптованој форми, тако да нико па ни сарадник за ИТ не може да их прочита.

У случају појаве безбедносног ризика, сарадник за ИТ има могућност да промени лозинке корисника.
Како лозинке корисника имају статус поверљивих података, ради спречавања безбедносних претњи и ризика услед откривања података за аутентификацију запослених, корисници ИКТ система Директората дужни су да:

- корисничко име и лозинку држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
- избегавају чување корисничког имена и лозинке у писаном облику;
- промене лозинку када примете да постоји било какав наговештај могућег компромитовања;
- не шаљу лозинке електронском поштом;
- одјаве се са ИКТ система по завршетку радних задатака.

За заштиту лозинки и других сопствених средстава за аутентификацију одговорни су сви корисници ИКТ система и то:

- запослени, у складу са овим Правилником, и
- трећа лица у складу са одговарајућим уговором.

Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података
Члан 17.

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

Криптозаштитом се обезбеђује:

- аутентификација (идентификација 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, који 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).

У оквиру ИКТ система, криптозаштита се користи уз поштовање следећих правила:

- енкрипција се користи за заштиту лозинки корисника на серверима, као и за удаљени приступ подацима у оквиру ИКТ система.
- минимална дужина енкрипционог кључа је 128-бит. Сигурност енкрипционог система веома зависи од тајности коришћених енкрипционих кључева.
- енкрипциони кључеви се не смеју слати путем е-*maila*.
- коришћење технологије јавних кључева захтева да се креира и одржава јавни и приватни кључ за сваког корисника.
- јавни кључеви се морају дистрибуирати или складиштити на такав начин који ће омогућити приступ само одређеним корисницима.

У оквиру система се користе следеће технологије енкрипције:

- *SSL (Secure Socket Layer)*, који је стандардни сигурносни протокол и користи асиметричну енкрипцију за аутентификацију и симетричну енкрипцију за заштиту комуникационих сесија. *SSL* се у Директорату користи за енкрипцију комуникације веб и е-маил сервиса;
- *IPSec* који се у организацији користи за успостављање ВПН тунела за спољне конекције на системе организације;
- SSH (Secure Socket) успоставља енкриптовани тунел између клијента и сервера, и користи се за удаљену администрацију сервиса и пренос података приликом спољних конекција;
- *WPA2 - PSK (AES) (WPA2: Wi-Fi Protected Access 2; PSK: Pre-Shared Key; AES: Advanced Encryption Standard)* протокол за услостављање конекција на системе путем *wireless* мреже.

Управљање кључевима
Члан 17а.

Директорат 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.

Управљање криптографским кључевима има следеће карактеристике:
- потпуно је аутоматизовано те запослени немају могућност утицаја на креирање кључа;
- подаци су заштићени јер се ниједан податак никада не појављује као чист текст када је енкриптован коришћењем кључа за енкрипцију кључева (кључ за енкрипцију кључева се користи за енкриптовање других кључева, што их штити од откривања);
- у зависности од потребе, кључеви се мењају најмање једном у три године.

Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документн ИКТ система и обрађују подацп у ИКТ систему
Члан 18.

Ради спречавања неовлашћеног физичког приступа просторијма у којима се налазе средства и документи ИКТ система, као и спречавања оштећења и ометања информација, просторије Директората су физички заштићене стандардним мерама заштите као што су закључавање просторија, употреба алармног система и видео-надзора.

Приступ просторијама и појединим зонама у Директорату се контролише и употребом идентификационих картица запослених.
Сва потребна опрема за безбедност физичког окружења се редовно одржава.

Зона раздвајања и успостављање система физичке безбедности
Члан 18а.

Опрема за обраду информација се штити закључавањем просторија у којима се налази, као и контролом приступа. У складу са проценом ризика постоје следеће зоне:
- серверска сала Директората;
- службене просторије са радним станицама и осталом ИКТ опремом;
- архивска просторија за документацију.

Серверска сала Директората је намењена за смештај сервера и мрежне опреме. Налази се у простору Директората и додатно је физички заштићена путем електричне браве са читачем картица и преградним вратима. Сала поседује електропроводни под и клима уређај који обезбеђује потребну температуру и влажност. Серверска сала је видно обележена и приступ је омогућен само овлашћеним лицима и то сараднику за ИТ, Шефу кабинета и директору путем идентифиационих картица за приступ.

Службене просторије са радним станицама и осталом ИКТ опремом су физички заштићене од неовлашћеног приступа помоћу врата са сигурносним бравама, видео надзором ходника и улаза у простор као и алармним системом са дојавом.

Архивска просторија за документацију је посебна зона у простору Директората која је намењена одлагању архивске документације. Ова просторија је заштићена од неовлашћеног приступа помоћу врата са сигурносном бравом и видео надзором постављеном ка улазу у просторију. Приступ је омогућен само овлашћеним лицима.

Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем
Члан 19.

Постављање и заштита опреме
Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа. Поред физичке заштите (механичке и електронске браве), алармног система и непрекидног видео-надзора, врши се редовна контрола система за обезбеђење, противпожарне заштите, као и инсталација за воду, струју и електронске комуникације. Све просторије и серверска сала поседују противпожарни апарат. Просторије са опремом се редовно чисте од прашине и редовно се прате температура и влажност ваздуха.

Сервери су заштићени од свих врста удара и физичких оштећења, од претерано високих или ниских температура, електромагнетних зрачења, као и од сувише високе или ниске влажности ваздуха. Сервери су монтирани у серверске ормане изнад пода како би се избегла оштећења у случају поплаве.

У серверској сали се редовно прате температура, влажност и други услови околине који би могли негативно да утичу на рад опреме за обраду информација.

Помоћне функције за подршку
Сервери и мрежна опрема у серверској сали користе уређаје за резервно напајење електричном енергијом (УПС) чији се рад прати а уређаји се благовремено сервисирају.

Безбедносни елементи приликом постављања каблова
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, када је то могуће, 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
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 уз надзор сарадника за ИТ;
- о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;
- осетљиве информације на неисправној опреми се уклањају из опреме;
- пре враћања опреме у рад након одржавања, сарадник за ИТ проверава да ли је опрема

неовлашћено коришћена или оштећена.

Периодично, а најмање једном годишње, се врши превентивни преглед ИТ опреме уз проверу температуре процесора, здравља носача података и других параметара.

Измештање и премештање имовине

Измештање и премештање рачунара са носачима података врши се непосредно од стране сарадника за ИТ или под његовом контролом, на следећи начин:

- непосредно од стране сарадника за ИТ унутар просторија Директората, у складу са Процедуром о приступу мрежи и мрежним услугама којом се омогућавају безбедносни механизми заштите измештене опреме;
- од стране запосленог изван просторија Директората, под контролом сарадника за ИТ, у складу са Процедуром о коришћењу мобилних уређаја којом се омогућавају безбедносни механизми заштите измештене опреме.

Измештање и премештање рачунарске опреме која нема носаче података врши се непосредно од стране сарадника за ИТ или под његовом контролом, на следећи начин:

- непосредно од стране сарадника за ИТ унутар просторија Директората, у складу са Процедуром о приступу мрежи и мрежним услугама;
- од стране трећих лица, под контролом сарадника за ИТ, за потребе сервисирања, у складу са уговором којим се омогућавају безбедносни механизми заштите измештене опреме.

Измештање и премештање софтвера и података врше сарадник за ИТ и/или надлежна трећа лица, у складу са уговором.

Безбедно расходовање или поновно коришћење опреме

Сарадник за ИТ проверава и процењује употребљивост коришћене опреме. У случају расходовања опреме која садржи медијуме за чување података, сарадник за ИТ спроводи верификацију како би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњени.

У случају да се опрема може поново користити, поступа се у складу са Процедуром о приступу мрежи и мрежним уређајима. Ако се делови опреме могу поново користити, они се уграђују у другу опрему и поступа се у складу са Процедуром о инсталацији и конфигурацији система.

Остављање осетљивих и поверљивих докумената и материјала

Сва осетљива и поверљива документа и материјали се уклањају са радне површине и одлажу на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе. У раду са осетљивим. поверљивим документима и материјалима (електронским или папирним), запослени је дужан да поступа у складу са процедуром за остављање осетљивих и поверљивих докумената и материјала.

Обезбеђивање исправног и бсзбедног функционисања средстава за обраду података
Члан 20.

Директорат је, у циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података дефинисао процедуре за руковање средствима за обраду података које садрже инструкције за детаљно извршење следећих послова:

1 Процедура о инсталацији и конфигурацији система;
2 Процедура за поступање, обраду, складиштење и пренос података;
3 Процедура за израду резервних копија;
4 Контакти за подршку, у случају неочекиваних оперативних или техничких потешкоћа су контакти са Сарадником за ИТ;
5 Инструкције за поступања према поверљивим подацима су дефинисане уговорима и изјавом о поверљивости;
6 Процедуре за поновно покретање система и опоравак, које се користе у случају отказа система се ради у складу са процедуром за укључивање и искључивање ссрвера.

У случају промене у организацији, пословним процесима и средствима за обраду информација и на системима које имају утицај на безбедност информација поступа се у складу са Процедуром о правима приступа ИКТ систему.
За усвајање, измене и допуне радних процедура овлашћен је директор.

Управљање расположивим капацитетима
Коришћење ИКТ ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходне перформансе система. Потребе за одржавањем и унапређењем система се исказују у оквиру Плана рада, Плана јавних набавки и Финансијског плана.

Периодично се спроводе следеће активности:
- брисање застарелих података које спроводи сарадник за ИТ (ако су подаци на серверима и не подлежу трајном чувању) и корисници (ако су подаци на радним станицама и не подлежу трајном чувању);
- повлачење из употребе апликација, система, база података или окружења и њихово архивирање;
- оптимизација серије процеса и распореда;
- одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нису критичне за пословање.

Раздвајање окружења за развој, испитивање и рад
Окружења за развој, испитивање и рад су међусобно раздвојена, како би се смањио ризик од неовлашћеног приступа или промена у радном окружењу.

Када год је то могуће, прави се тестно окружење које је одвојено од оперативног и не садржи осетљиве податке из ИКТ система.

Трећа лица која учествују у изради или развоју софтвера за потребе Директората, у сарадњи са Сарадником за ИТ, документују правила за преношење софтвера из развојног или модификованог статуса у оперативни статус.

Смернице за раздвајање окружења за развој, испитивање и рад су:
- развојни и радни софтвери треба да се извршавају на различитим системима или рачунарским процесорима, као и у различитим доменима или директоријумима;
- промене у радним системима и апликацијама треба да се испитују у тестном окружењу или у режиму одржавања пре него што се примене на радне системе;
- испитивање се не ради на радним верзијама система, осим у изузетним околностима;
- компајлери, едитори и други развојни алати или системски помоћни програми не треба да буду доступни из оперативних система, ако се то не захтева;
- осетљиви подаци се не копирају у системско тестно окружење, осим ако нису

обезбеђене еквивалентне контроле за систем за испитивање.

Заштита података и средстава 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 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 21а.

Директорат, у циљу заштите од злонамерног софтвера, одређује и примењује мере контроле ради његовог откривања и спречавања, као и опоравка од штетног дејства злонамерног софтвера у складу са Процедуром о заштити од злонамерног софтвера.

Мере из става 1. овог члана Правилника укључују:
- проверу, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер;
- проверу, пре коришћења, садржаја прилога електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер;
- проверу постојања злонамерних софтвера на веб-страницама;
- 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;
- припрему одговарајућих планова за континуитет пословања приликом опоравка од напада злонамерним софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак;
- редовно прикупљање информација о новим злонамерним софтверима
  као што је претплата на адресне спискове за доставу или провера веб-страница на којима се дају информације о новим злонамерним софтверима;

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

У циљу заштите од упада у ИКТ систем, сарадник за ИТ је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе интернета, сарадник за ИТ може укинути приступ.

Заштита од губитка података
Члан 22.

Директорат спроводи израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација и података
Члан 22а.

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују у складу са Процедуром за израду резервних копија.

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 околности.

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.

Израда и чување резервних копија одвија се унутар централног ИКТ система Директората на специјализованим серверима *(backup storage server)* а затим се заштићеном енкриптованом везом синронизују на удаљену локацију која је под мерама заштите ИКТ система Директората.

У циљу израде и испитивања резервне копије информација, софтвера и дупликати система, сарадник за ИТ 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.

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система
Члан 23.

У оквиру ИКТ система Директората формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Записивање догађаја
Члан 23а.

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;

- датотеке којима се приступало и врсте приступа;
- мрежне адресе и протоколе;
- активирање и деактивирање система заштите, као што су антивирусни системи и системи за откривање упада.

Заштита информација у записима
Члан 23б.

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

Записи администратора и оператора
Члан 23в.

Активности администратора и оператора система се записују, а записи се штите и редовно преиспитују.

Сатови свих одговарајућих система за обраду информација заштите морају бити синхронизовани са средњим временом по Гриничу.

За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужен је сарадник за ИТ.

Обезбеђивање интегритета софтвера и оперативних система
Члан 24.

Директорат спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за контролу промена и инсталацију софтвера.

Смернице за контролу промена и инсталацију софтвера су:
- ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљени администратори или трећа лица по основу уговора, уз надзор сарадника за ИТ;
- апликације и оперативни системски софтвер се имплементира након успешно спроведеног испитивања, које обухвата испитивање применљивости, безбедности, утицаја на друге системе и погодности за коришћење, а спроводи се у тестном окружењу;
- пре имплементације било каквих промена, успоставља се стратегија повратка на претходно стање;
- приликом свих ажурирања на библиотекама оперативних програма, одржавају се записи за проверу;
- као мера предострожности за неочекиване ситуације чувају се претходне верзије апликативног софтвера;
- старије верзије софтвера се архивирају, заједно са свим потребним информацијама и параметрима, процедурама, детаљима конфигурације и софтвером за подршку, све док се подаци држе у архиви.

У ИКТ систему може да се инсталира само софтвер и оперативни системи за који постоји важећа лиценца у власништву Директората.

Инсталацију и подешавање софтвера може да врши само сарадник за ИТ и трећа лица у складу са уговором.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система
Члан 25.

Директорат 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 25а.

Сарадник за ИТ најмање једном месечно, а по потреби и чешће прати рад ИКТ система и врши анализу дневника активности (*activitylog, history, securitylog, transactionlog* и др) у циљу идентификације потенцијалних слабости ИКТ система.

Сарадник за ИТ, такође повремено врши периодичне тестове безбедности ИКТ система како би идентификовао слабости у безбедносним процедурама ИКТ система. Ови тестови обухватају све сегменте ИКТ система. Приликом спровођења тестирања, води се рачуна да ове активности не утичу на нормално функционисање система, или да њихов утицај буде минимализован.

У складу са процењеним рањивостима и у договору са одговарајућим трећим лицима задуженим за имплементацију или одржавање по основу уговора, сарадник за ИТ предузима мере и акције у намери исправке рањивих делова ИКТ система, а све у циљу смањивања безбедоносних ризика и спречавања злоупотребе техничких безбедносних слабости ИКТ система. Акције које се могу спровести су: едукација, измена процедура рада, измена постојећих верзија софтвера, или набавка нових (хардвера, софтвера, услуга, система и сл.).

Сарадник за ИТ са надређенима процењује и у зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, предузима активност које су везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности.

Управљање техничким рањивостима се усклађује са активностима које се односе на управљање инцидентима, тако да се обезбеди примена процедура које треба спровести ако се догоди неки инцидент.

Ограничења у погледу инсталације софтвера
Члан 25б.

Инсталирање софтвера врши сарадник за ИТ и одговарајућа трећа лица у складу са уговором. Осталим лицима је забрањена инсталација софтвера у ИКТ систему Директората.

Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система
Члан 26.

Приликом спровођења ревизије ИКТ система, Директорат се стара да ревизија има што мањи утицај на функционисање система.

Поступак ревизије информационих система подразумева:

- да су са руководством Директората договорени захтеви за проверу приступа систему и подацима;
- да су предмет и подручје испитивања за проверу унапред договорени и строго контролисани;
- да су испитивања за проверу показала да поступак ревизије информационих система може утицати на доступност система, па се покреће ван радног времена;
- да се сваки приступ надгледа и записује да би се направио референтни траг.

Планирање и спровођење ревизије ИКТ система може да врши само сарадник за ИТ, односно запослени који има овлашћење за то.

Заштита података у комуникационим мрежама укључујући уређаје и водове
Члан 27.

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

Приступ мрежи и мрежној опреми спроводи се уз обавезан надзор сарадника за ИТ, који је дужан да константно врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система
Члан 28.

Заштита података који се размењују комуникационим средствима унутар ИКТ система Директората, или са другим ИКТ системима организација или трећих лица, обезбеђена је интерним процедурама, уговорима и споразумима са организацијама и трећим лицима, као и применом адекватних контрола.

Правила коришћења електронске поште
Употреба електронске поште врши се у складу са Процедуром о безбедности у размени електронских порука. Електронска пошта се може користити искључиво за пословне потребе и размена порука личног садржаја није дозвољена. Сви подаци садржани у порукама или њиховом прилогу су у складу са стандардима заштите података.

Правила коришћења интернета
Приступ садржајима на интернету је дозвољен искључиво за пословне намене. Сарадник за ИТ периодично спроводи поступак ревизије и контролисања логовања, како на пријему тако и на слању.
Забрањена је употреба веб сајтова са неприкладним садржајем, друштвених мрежа, интернет форума, сајтова за клађење, преузимање музике, филмова и осталих садржаја који нису у вези са обављањем послова из надлежности Директората

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 28а.

Безбедан пренос пословних и интерних информација између Директората и трећих лица обезбеђују су у складу са другим посебним законима и уговорима.

Питања информационе безбедности у оквиру управљаља свим фазама животног циклуса ИКТ система односно делова система
Члан 29.

Стандарди информационе безбедности постављају се у оквиру сваке фазе развоја ИКТ система Директората, а нарочито током фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и повлачења из употребе.

Развој новог или замена постојећег дела ИКТ система се увек реализује у складу са планом набавки или у оквиру пројеката.

Сарадник за ИТ, односно запослени кога овласти директор 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, сарадник за ИТ 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 безбедност информација
Члан 29а.

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

Захтеви за безбедност информација 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 мора узети у обзир аутоматску контролу која ће бити уведена у информациони систем и потребу да такође постоји и ручна контрола, која мора бити примењена при вредновању пакета софтвера, развијених или купљених, 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 се примењује за нове као и за модификоване делове ИКТ система. У уговору са трећим лицима се дефинишу се захтеви безбедности.

Обезбеђивање апликативних услуга у јавним мрежама
Члан 29б.

Информације обухваћене апликативним услугама које пролазе кроз јавне мреже се штите од малверзација, неовлашћеног откривања података и модификовања, у складу са интерним правилима и процедурама, уговорима и споразумима са организацијама и трећим лицима, као и применом адекватних контрола.

Потврда идентитета корисника, подела овлашћења и одговорности за постављање садржаја, електронског потписивања или обављања трансакција су у складу са радним задацима запосленог и садржани су у креденцијалима који су му додељени.

Заштита трансакција апликативних услуга
Члан 29в.

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.

Енкриптовање података се користи приликом коришћења ВПН приступа или комуникације преко портала, док се безбедност у размени електронских порука постиже Процедуром о безбедности у размени електронских порука.

Заштита података који се користе за потребе тестирања ИКТ система односно делова система
Члан 30.

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

Тестирање ИКТ система односно делова система могу да врше одговарајућа трећа лица у складу са уговором који садржи клаузулу о поверљивости података, сарадник за ИТ или други запослени, овлашћен од стране директора.

За потребе испитивања и тестирања ИКТ система, односно делова система, Директорат избегава коришћење оперативних пословних и интерних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачну личност.

Уколико је за тестирање неопходно користити оперативне податке, тада се примењују следеће мере безбедности:
за свако копирање оперативних података у тестно окружење се издаје посебно овлашћење;

- за потребе тестирања ИКТ система односно делова система, се користе подаци који нису осетљиви;
- уколико се за сврху испитивања користе лични подаци или неке друге поверљиве или осетљиве информације, онда се користи метода „измишљене особе“ чији подаци нису стварни али симулирају стварне;
- уколико се за сврху испитивања морају користити лични подаци тада се свако

копирање оперативних података у тестно окружење врши се под надзором сарадника за ИТ а у складу са уговором;
- сарадник за ИТ, или други запослени, овлашћен од стране директора, као и трећа лица дужни су да штите, чувају и контролишу податке у тестном окружењу на одговарајући начин;
- оперативне информације се одмах по завршетку испитивања бришу из тестног окружења.

Приликом тестирања апликативних система примењују се додатне мере за контролу приступа путем физичке заштите и применом криптографских мера за заштиту система и података од неовлашћених приступа, које се примењују и на оперативним системима.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга
Члан 31.

Ниво приступа и безбедносни стандарди који су неопходни како би се одговарајућим трећим лицима омогућио приступ подацима, информацијама, средствима или опреми за обраду информација ИКТ система, регулишу се уговорима између Директората и трећих лица. Такви уговори садрже уговорну клаузулу о заштити и чувању поверљивости информација, података и документације Директората.

Директорат успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга.

Уговарање обавезе обезбеђивања безбедности у споразумима са пружаоцима услуга
Члан 31а.

Пре отпочињања преговора, потенцијални пружалац услуга Директорату у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, 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 Директората, а за потребе извршења предмета преговора.

Изјава 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 Директората, у случају повреде ове одредбе.

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

Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга
Члан 32.

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

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга
Члан 32а.

Пружалац услуге има уговорну обавезу да организује и припреми периодичне састанаке који ће обезбедити редовно извештавање Директората и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене.

Сарадник за ИТ или овлашћена особа у Директорату редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

- обезбеђује неопходност поштовања свих услова из споразума у вези са безбедношћу информација, а нарочито спречавања свих инцидената и проблема нарушавања безбедности, те омогућавања управљања на одговарајући начин;
- врши ~~ее~~ оцену квалитета извршења и саобразности уговорене услуге;
- 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;
- одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања;
- преиспитује трагове провере и записа о догађајима у вези са безбедношћу код пружаоца услуга, односно оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.
- по потреби, надгледање и преиспититује извршење услуге ангажовањем трећег лица.

Управљање променама уговорених услуга од стране пружаоца услуга
Члан 32б.

Уговором са пружаоцем услуга се обезбеђује 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 Директорат 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 33.

Процедуром за управљање безбедносним инцидентима у ИКТ систем се уређује начин одговора на инциденте нарушавања безбедности информација, и сарадник за ИТ је особа за контакт у случајевима нарушавања безбедности, као и контакте са овлашћеним телима.

Сарадник за ИТ има задатак да придржавајући се процедура одређених овим чланом, детектује, анализира и информише надлежне у току и након инцидента.

Сарадник за ИТ у циљу превенције од безбедносних ризика обезбеђује више (различитих и другачијих) мехнизама за комуникацију и координацију у случају нарушавања безбедности. У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени је дужан да о томе одмах обавести сарадника за ИТ и надређене.

Сарадник за ИТ води евиденцију о свим инцидентима, као и пријавама инцидената.

Одговор на инциденте нарушавања информационе безбедноости
Члан 33а.

Директорат је у обавези да усвоји План за превенцију од безбедносних ризика.

План за превенцију од безбедносних ризика садржи одговоре на питања ко, када и како треба да буде контактиран и које акције треба предузети моментално у случају одређеног напада. План из става 2. овог члана Правилника нарочито садржи:

- класификациону шема – детаље о подацима који се налазе у систему, њихов ниво осетљивости и поверљивости.
- листу услуга – попис свих услуга које Директорат пружа, рангиране по важности.
- план за прављење резервних копија и повраћај података – дефинише за које податке се раде резервне копије, носаче података на које ће се снимати, где се носачи чувају и колико често се праве резервне копије и поступак за повраћај података.
- план за замену опреме односно списак потребне опреме, рангиране по важности.

Прикупљено знање из анализе и решавања инцидената који су нарушили информациону безбедност, Директорат користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

Прикупљање доказа
Члан 33б.

Директорат дефинише и примењује процедуре за идентификацију, сакупљање, набавку и чување информација које могу да послуже као доказ у случају покретања дисциплинског, прекршајног или кривичног поступка.

Мере које обезбеђују континуитет обављања посла у ванредним околностима
Члан 34.

Директорат примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

Континуитет пословања се осигурава кроз План за обезбеђење континуитета пословања и План опоравка од нежељених догађаја ИКТ система.

Имплементација континуитета безбедности информација
Члан 34а.

Сарадник за ИТ 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

Члан 35.

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

Члан 36.

Ступањем на снагу овог Правилника престаје да важи Правилник о употреби информатичке опреме и информационог система и поступању са информацијама и документима од 19. јула 2019. године.

Ступање на снагу Правилника о безбедности информационо-комуникационог система

Члан 37.

Овај Правилник ступа на снагу осмог дана од дана објављивања на огласној табли Директората.

У Београду, 08. септембар 2023. године
Број: 110-00-4/2023-02

ЗАМЕНИК ПРЕДСЕДНИЦЕ ОДБОРА

Др Владимир Удовичић, доктор физичких наука