На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, бр. 6/16, 97/17) и Закона о изменама и допунама Закона о информационој безбедности „Службени гласник РС”, број 77/19), те 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), као и чл. 16. и 24. Покрајинске скупштинске одлуке о покрајинској управи („Службени лист АП Војводине”, бр. 37/2014, 54/2014 – др. одлука, 37/2016 и 29/2017, 24/2019 и 66/2020), покрајинска секретарка за финансије доноси

Правилник о безбедности информационо-комуникационог система *BISTrezor* Покрајинског секретаријата за финансије

I. ОСНОВНЕ ОДРЕДБЕ

Предмет

Члан 1.

Правилником о безбедности информационо-комуникационог система *BISTrezor* Покрајинског секретаријата за финансије (у даљем тексту: Правилник) детаљније се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности, као и овлашћења и одговорности у вези с безбедношћу и ресурсима информационо-комуникационог система Покрајинског секретаријата за финансије, који развија Сектор за информациони систем буџета и трезора (у даљем тексту: Сектор) Покрајинског секретаријата за финансије (у даљем тексту: Секретаријат), за потребе планирања и извршења буџета Аутономне покрајине Војводине (у даљем тексту: АП Војводина) и представља интегрисани информациони систем буџета и трезора АП Војводине (у даљем тексту: систем *BISTrezor*).

Одредбе овог правилника односе се на запослене код директних и индиректних корисника буџета АП Војводине, који у обављању послова свог радног места користе систем *BISTrezor* (у даљем тексту: корисници система *BISTrezor*).

Члан 2.

Све именице које се у овом правилнику користе у мушком роду, а имају и женски род, подразумевају и истовремено обухватају исте именице у женском роду.

Именице које означавају службене позиције и функције користе се у облику који изражава пол лица које је њихов носилац.

Циљеви Правилника

Члан 3.

Циљеви доношења Правилника јесу:

1) одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система *BISTrezor*;
2) спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност система *BISTrezor*;
3) подизање свести корисника система *BISTrezor* о значају информационе безбедности, као и о ризицима и мерама заштите приликом коришћења *BISTrezor* система;
4) прописивање овлашћења и одговорности корисника система *BISTrezor* у вези с безбедношћу и ресурсима система *BISTrezor*;
5) свеукупно унапређивање информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Правилника

Члан 4.

Мере заштите система *BISTrezor*, које су детаљније уређене Правилником, служе превенцији настанка инцидената и минимизацији штете од инцидената, а њихова примена обавезна је за све кориснике система *BISTrezor*.

Корисници система *BISTrezor* дужни су да се придржавају одредаба Правилника, као и других интерних процедура које регулишу информациону безбедност. Правилник и релевантне процедуре биће доступне корисницима у оквиру система *BISTrezor*.

Приликом попуњавања захтева за доделу права, сваки корисник система *BISTrezor* дужан је да дâ писмену изјаву (или изјаву потписану верификованим електронским потписом), којом потврђује да је упознат са садржином Правилника. Изглед и садржај изјаве дати су у процедури „Додељивање права запосленом за рад на појединачним деловима система *BISTrezor*", која је саставни део система *BISTrezor*.

Руководилац Сектора и начелник Одељења за израду и одржавање информационог система (у даљем тексту: Одељење) одговорни су за праћење примене мера безбедности система *BISTrezor*, као и за проверу тога да ли су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност корисника система *BISTrezor*

Члан 5.

Сваки корисник система *BISTrezor* одговоран је за безбедност података ресурса које користи ради обављања послова из своје надлежности у оквиру система *BISTrezor* и дужан је да благовремено информише Интерни ЦЕРТ система *BISTrezor* на имејл адресу cert.bistrezor@vojvodina.gov.rs о свим сигурносним инцидентима и проблемима.

Кориснику система *BISTrezor* који наруши информациону безбедност и угрози функционисање система *BISTrezor* може да се суспендује право на рад у систему *BISTrezor* на одређено време.

Кориснику система *BISTrezor* који поново наруши информациону безбедност и угрози функционисање система *BISTrezor* може трајно да се одузиме право на рад у систему *BISTrezor*.

Предмет заштите

Члан 6.

Мере заштите система *BISTrezor* односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља системом *BISTrezor*, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Предмет заштите јесу :

- главни сервер;
- резервни сервер;
- тестни сервер;
- база података;
- програмски кодови система *BISTrezor*.

II. МЕРЕ ЗАШТИТЕ

Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу система *BISTrezor* у оквиру Секретаријата

Члан 7.

Секретаријат – у оквиру организационе структуре – утврђује послове и одговорности запослених у Сектору с циљем управљања информационом безбедношћу.

Интерни акти који уређују обавезе и одговорности запослених Сектору у вези са управљањем информационом безбедношћу система *BISTrezor*:

- акт о организацији и систематизацији радних места;
- акт о заснивању радног односа (нпр. решење о распоређивању, уговор о раду);
- уговори о чувању поверљивости с правним лицима;
- решење о одређивању лица за приступ посебно осетљивим подацима и информацијама у систему *BISTrezor*.

Руководилац Секретаријата дужан је да донесе појединачни акт којим се дефинише оснивање Центра за превенцију безбедносних ризика у ИКТ систему Секретаријата (у даљем тексту: Интерни ЦЕРТ), као и акт којим се – у складу са актом о организацији и систематизацији радних места – одређују запослени, чланови Интерног ЦЕРТ-а, да обезбеђују и прате безбедност информационог система *BISTrezor*.

Процедуром за „Додељивање права запосленом за рад на појединачним деловима система *BISTrezor*" утврђују се начин доделе овлашћења и начин одобравања приступа за рад у систему *BISTrezor*.

Захтев за доделу права – који потписује руководилац корисника система *BISTrezor* – доставља се на прописаном обрасцу који је саставни део процедуре за „Додељивање права запосленом за рад на појединачним деловима система *BISTrezor*".

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 8.

Под мобилним уређајима подразумевају се сви преносни електронски уређаји намењени за комуникацију на даљину.

У мобилне уређаје сврставају се преносиви рачунари, таблети, мобилни телефони, *PDA* и сви други мобилни уређаји који садрже поверљиве податке и имају могућност повезивања на мрежу АП Војводине.

Приликом коришћења мобилних уређаја, потребно је осигурати пословне информације од могућег компромитовања.

Администратор система *BISTrezor* утврђује начин и дозвољава рад на даљину и употребу мобилних уређаја, 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, заштитита од крађе и активности које је неопходно предузети у случају крађе или губитка мобилних уређаја како не би била нарушена безбедност.

Рад на даљину и коришћење мобилних уређаја

Члан 9.

Обављање послова ван службених просторија корисника система *BISTrezor* обухвата:

- рад на даљину;
- рад од куће;
- виртуелно радно окружење.

Такође, рад на даљину – у смислу овог правилника – односи се на ситуацију када је корисник система *BISTrezor* и друго радно ангажовано лице обавезано да изврши одређене послове у систему *BISTrezor*, а налази се ван службених просторија. Предметно ангажовање и омогућавање обављања задатих и неопходних послова уређује се путем Процедуре за VPN приступ информационом систему (у даљем тексту: VPN процедура).

VPN приступ информационом систему одобрава и омогућује Управа за заједничке послове покрајинских органа, на основу захтева директног буџетског корисника.

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

Члан 10.

Системом *BISTrezor* управљају запослени у Сектору – у складу с важећим актом о систематизацији радних места.

Сектор је дужан да сваког новог корисника система *BISTrezor* упозна са одговорностима и правилима коришћења система *BISTrezor*, као и да води евиденцију о изјавама којима корисници система *BISTrezor* потврђују да су упознати са садржајем Правилника и с правилима коришћења система *BISTrezor*.

Свако коришћење система *BISTrezor* од стране корисника система BISTrezor и запослених у Сектору, ван додељених овлашћења, подлеже дисциплинској одговорности – у складу с важећим законима и с Кодексом понашања службеника и намештеника у органима АП Војводине.

Обавезе у току коришћења система BISTpezor

Члан 11.

Сви корисници система *BISTpezor* у обавези су да примењују мере заштите безбедности, у складу с Правилником и важећим процедурама.

Ради развоја, имплементације и одржавања система заштите и безбедности података система *BISTrezor*, Сектор обезбеђује услове за интеграцију контролних механизама тако што:

- обезбеђује да се поступци заштите спроводе на организован начин и у складу с процедурама и у континуитету;
- спроводи програме заштите на конзистентан и уједначен начин код свих корисника система *BISTrezor*;
- координира безбедност и заштиту података у информационом систему *BISTrezor* с њиховом физичком заштитом.

Запослени у Сектору, који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура, континуирано се обучавају ради унапређивања техничког и технолошког знања. Руководилац Сектора и чланови Интерног ЦЕРТ-а ауторизовани су за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију система *BISTrezor*, који су под мерама заштите.

Упознавање с безбедношћу информација, стицање знања и обука

Члан 12.

Запослени у Сектору и чланови Интерног ЦЕРТ-а у обавези су да прођу одговарајућу обуку и да редовно стичу нова и обнављају постојећа знања о процедурама и другим актима, који уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Заштита од ризика који настају при променама послова или приликом престанка радног ангажовања лица у Секреатријату и лица који користе систем *BISTrezor*

Члан 13.

Запослени у Сектору и лица која је Секретаријат ангажовао по другом основу, дужни су да чувају поверљиве и друге информације које су значајне за информациону безбедност система *BISTrezor* и након промене радног места, односно након престанка радног односа или радног ангажовања.

Дужности и обавезе које остају важеће у случају из става 1. овог члана дефинишу се решењем о именовању чланова Интерног ЦЕРТ-а и решењем о праву на заједничке идентификаторе.

Кориснику система *BISTrezor* који прелази на друго радно место укида се право рада у систему *BISTrezor* и могу му се одобрити нова права у зависности од новоутврђених послова, у складу с процедуром „Додељивање права запосленом на рад на појединачним деловима система *BISTrezor*". Процедура је постављена у систему *BISTrezor*, у падајућем менију *Proc. i uputstva*. Рок за укидање права јесте три дана од доношења акта о преласку на друго место.

Престанком радног односа или радног ангажовања, кориснику система *BISTrezor* укидају се сва права на рад у систему *BISTrezor*. Та права укидају се одмах по доношењу акта о престанку радног ангажовања. Укидање права на рад у систему BISTrezor даје руководилац, попуњавањем обрасца захтева за укидање права, што се евидентира у посебној евиденцији.

У случају престанка радног односа запосленог у Сектору, обавезе Сектора су следеће:

- да прегледа све налоге и приступе систему *BISTrezor*, који су били доступни запосленом;
- да провери садржај враћених мобилних уређаја и уређаја за преношење података који су коришћени за рад у систему *BISTrezor* и – по потреби – да тај садржај избрише;
- да запосленом укине право приступа систему *BISTrezor* на дан престанка радног односа или другог основа ангажовања тог запосленог;
- да прегледа све налоге за приступ запосленог систему *BISTrezor* и да прикупи приступне шифре и кодове с циљем њиховог укидања/промене на дан одласка.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 14.

Информациона добра система *BISTrezor* обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компоненти, програмске захтеве и техничку документацију у коју се сврставају писана упутства, пројектна документација и процедуре.

Пописивање имовине

Члан 15.

Сектор 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.

Сектор прави попис информационих добара Секретаријата, који је тачан, ажуран, конзистентан и усклађен с другом имовином.

Евиденцију о информационим добрима води Интерни ЦЕРТ.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај

Члан 16.

Интерни ЦЕРТ има одговорност за контролисање животног циклуса информационих добара система *BISTrezor* и дужан је да правилно управља информационим добрима током целог животног циклуса.

Интерни ЦЕРТ-а даје препоруке за правилно коришћење имовине повезане са информацијама и опремом за обраду информација.

Запослени у Сектору и екстерни сарадници обавезни су да врате сву имовину коју поседују након престанка њиховог запослења или радног ангажовања.

Класификовање података

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

Члан 17.

Класификовање података јесте поступак утврђивања и појединачног додељивања нивоа тајности податка, у складу с њиховим значајем за Секретаријат.

Секретаријат означава типове и локације података као поверљиве, интерне или јавне.

Класификациону шему поверљивости информација Секретаријат дефинише на основу права рада у систему *BISTrezor*:

- право на основу доделе права;
- право на основу рада у Сектору (основна права – тестни подаци);
- решење о одређивању лица за приступ посебно осетљивим подацима и информацијама у систему *BISTrezor*.

Секретаријат врши класификацију ради:

- јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и буду свесни одговорности за неовлашћено коришћење или преношење;
- подизања свести о вредности информације или документа;
- заштите података у покрету ради боље и интелигентније интеграције са *DLP, WEB gateway* и осталим производима за заштиту параметара и крајњих уређаја;
- заштите садржаја;
- интеграције са системима за архивирање.

Класификација документа усклађена је с правилима контроле приступа.

Секретаријат поступа у складу са усвојеном шемом класификовања података. Посебним процедурама, дефинишу се радње за поступање, обраду, складиштење и пренос података.

Заштита, управљање и расходовање носача података

Члан 18.

Сектор обезбеђује спречавање неовлашћеног модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци води Интерни ЦЕРТ.

Сектор је дужан да за управљање преносним носачима података развија и имплементира процедуру о управљању преносним носачима, у складу са усвојеном шемом класификовања података.

Сектор врши безбедносно расходовање носача података, уз свођење на минимум ризика од доласка осетљивих информација до неовлашћених особа.

Безбедносно расходовање носача података врши се у складу с Процедуром за безбедносно расходовање носача података.

Физички пренос носача података (медијума)

Члан 19.

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

Секретаријат ће обезбедити сигурну и безбедну локацију за чување података система *BISTrezor*.

Подаци ће се на другу локацију преносити на сигуран и безбедан начин.

Ограничење приступа подацима и средствима за обраду података

Члан 20.

Приступ подацима и средствима за обраду података у систему *BISTrezor* ограничен је у складу са утврђеним степеном тајности података и усвојеном шемом класификовања података према члану 17. овог правилника.

Сектор ће формирати контролну листу приступа, која садржи попис свих информационих објеката и субјекте који им могу приступити.

Корисницима система *BISTrezor* дозвољен је приступ само само у оквиру права додељених корисничким налогом.

Запослени у Сектору, који има администраторски налог, има права приступа свим ресурсима система *BISTrezor* (софтверским и хардверским, мрежи и мрежним ресурсима) ради инсталације, одржавања, подешавања и управљања ресурсима система *BISTrezor*.

Корисник система *BISTrezor* може да користи само свој кориснички налог који је добио од администратора и не сме да омогући другом лицу коришћење његовог корисничког налога, сем администратору за подешавање корисничког профила и радне станице.

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа систему *BISTrezor* и услугама које систем пружа

Члан 21.

Сектор управља приступом систему *BISTrezor* и услугама употребом корисничких идентификатора.

Управљање корисничким идентификаторима врши се поштујући следеће принципе:

- кориснички идентификатори су јединствени и треба да омогуће да подаци буду заштићени од неовлашћеног приступа, као и да се заштите интегритет, расположивост, аутентичност и непорецивост тих података, да би систем *BISTpezor* функционисао како је предвиђено;
- коришћење заједничких идентификатора дозвољава се само онда када је то потребно за обављање посла, у складу с решењем о одређивању лица за приступ посебно осетљивим подацима и информацијама у систему *BISTrezor*, које доноси руководилац Секретаријата. Заједнички идентификатори се овим решењем могу доделити само запосленима у Сектору и лицима која је ангажовао Секретаријат. Заједнички идентификатори су с највишим правом приступа у шеми класификовања права;
- корисницима којима је престао радни однос или радно ангажовање онемогућава се рад у систему *BISTrezor* и уклањају им се кориснички идентификатори.

Право приступа систему *BISTrezor* додељује се кориснику система *BISTrezor* на основу захтева који је потписало овлашћено лице, у складу с радним задацима које обавља. Кориснику система *BISTrezor* додељују се јединствени подаци и јединствена шифра за логовање, који се не смеју делити с другим лицима.

Додељивање привилегованих (администраторских) права за приступ систему *BISTrezor* врши се на основу посебног решења о одређивању лица за приступ посебно осетљивим подацима и информацијама у систему *BISTrezor*, које је потписао руководилац Секретаријата. Привилегована права за приступ систему *BISTrezor*, која треба доделити администратору, другачија су од оних која се користе за редовне активности.

Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора.

Шифре за приступ заједничким корисничким идентификаторима администратора система *BISTrezor* мењају се када се промени барем један администратор.

Приступ свим ресурсима система *BISTrezor* имају запослени у Сектору, са администраторским привилегијама.

Право приступа систему *BISTrezor* корисник система *BISTrezor* добија по додели права. Корисници система *BISTrezor* морају поднети захтев за доделу права за приступ и захтев за инсталацију система *BISTrezor*. Захтеви – које потписује непосредни руководилац – подносе се Сектору, у складу с потребама обављања пословних задатака. Након одобравања захтева, датом кориснику се отвара кориснички налог и инсталира се систем *BISTrezor*. Уколико је захтев са ограниченим трајањем, право приступа кориснику се аутоматски укида истеком периода на захтеву.

Корисницима система *BISTrezor* и екстерним сарадницима по престанку запослења или истека ангажовања укида се право на приступ.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 22.

Кориснички налог састоји се од корисничког имена и лозинке.

Корисничко име формира се од латиничких слова имена или имена и презимена.

Администратор система *BISTrezor* додељује кориснику система *BISTrezor* иницијалну лозинку, коју је дужан да промени.

Лозинка треба да садржи велика и мала слова и цифре. Лозинка не треба да садржи препознатљиве податке о кориснику система *BISTrezor* (нпр. у виду имена, презимена, датума рођења).

Корисник система *BISTrezor*, коме је додељен кориснички налог, дужан је да га чува у најстрожој тајности, тако да га само он зна. Ако корисник система *BISTrezor* посумња да је друго лице открило његову лозинку, дужан је да ту лозинку одмах измени. Неовлашћено уступање корисничког налога другом лицу подлеже дисциплинској одговорности.

Систем *BISTrezor* периодично, а најмање четири пута годишње, од корисника система *BISTrezor* захтева да промени своју лозинку.

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

Члан 23.

Приступ ресурсима система *BISTrezor* не захтева посебну криптозаштиту.

Управљање кључевима

Члан 24.

Корисници система *BISTrezor* могу да користе своје квалификоване електронске сертификате за електронско потписивање докумената. Такви документи могу бити саставни део података који се обрађују у систему *BISTrezor*.

За инсталацију потребног софтвера и хардвера за коришћење личних електронских сертификата на корисничким радним станицама задужена је Управа за заједничке послове покрајинских органа.

Корисници система *BISTrezor* дужни су да чувају своје електронске сертификате како не би доспели у посед других лица.

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

Члан 25.

Сектор је дужан да предузме мере ради спречавања неовлашћеног физичког приступа систем-сали у којој се налазе средства и документи система *BISTrezor*, као и спречавања оштећења и ометања информација и опреме за обраду информација.

Зона раздвајања и успостављање система физичке безбедности

Члан 26.

Опрема за обраду информација штити се закључавањем просторија у којима се налази.

Контрола физичког уласка

Члан 27.

Простор у којем се налази опрема система *BISTrezor* обезбеђује се механичком бравом и магнетном картицом.

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

Члан 28.

Управа за заједничке послове покрајинских органа простор у коме се налази опрема система *BISTrezor* обезбеђује од пожара и других елементарних непогода.

Рад у безбедним зонама

Члан 29.

Систем-сала је простор у коме се налазе сервери, мрежна или комуникациона опрема система и представља безбедносну зону.

Простор је обезбеђен од пожара и других елементарних непогода и у њему је одговарајућа температура (климатизован простор).

Безбедна зона подлеже следећим мерама заштите:

- руководилац Сектора или начелник Одељења мора бити обавештен о постојању и активностима унутар безбедне зоне;
- забрањен је рад без надзора;
- безбедна зона је физички закључана;
- не дозвољава се уношење фотографских, видео-уређаја и аудио-уређаја или других уређаја за записивање, осим уз претходно одобрење руководиоца Сектора или начелника Одељења.

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

Постављање и заштита опреме

Члан 30.

Опрема се поставља и штити тако да се смањује ризик од претњи и опасности из окружења, као и могућности за неовлашћени приступ.

Руководилац Сектора и начелник Одељења редовно прате 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 31.

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 поправљају кварови;
- обезбеђује вишеструко напајање с различитих траса; сервери су непрекидно прикључени на *SMART* уређаје за непрекидно напајање и на агрегатску електричну мрежу.

Безбедносни елементи приликом постављања каблова

Члан 32.

Управа за заједничке послове покрајинских органа стара се о безбедности приликом постављања активне и пасивне мрежне опреме.

Одржавање опреме

Члан 33.

Како би се осигурала непрекидна расположивост и неповредивост опреме, одржава се на следећи начин:

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

Измештање и премештање имовине

Члан 34.

Опрема, информације или софтвер измештају се само уз одобрење руководиоца Сектора и начелника Одељења, а током измештања, примењују се следећа правила:

- за измештање опреме постављају се временска ограничења и проверава се усклађеност приликом повратка;
- захтевом за измештање опреме из систем-сале, документују се идентитет и улога лица која користе или која поступају са имовином приликом премештања и та документација треба да буде враћена са опремом, информацијама или софтвером.

Безбедност измештене опреме и имовине

Члан 35.

Изношење опреме ради селидбе, сервисирања, капиталног одржавања просторије и слично, спроводи се на основу захтева начелника Одељења за измештање опреме из систем-сале, који одобри руководилац Сектора. Захтев садржи списак опреме која се износи, услове под којима се износи, начин изношења и место њеног привременог или трајног смештања.

Опрема из просторије се изузетно, у случају опасности од пожара, временских непогода и слично, може изнети и без одобрења руководиоца Сектора.

Приликом изношења опреме ради сервисирања, сачињава се записник који садржи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Уговором са сервисером ће бити дефинисане обавезе заштите података који се налазе на медијима који су део система *BISTrezor* ресурса Секретартијата.

Безбедно расходовање или поновно коришћење опреме

Члан 36.

Сви делови опреме који садрже медијуме за чување података се прегледају, да би се сви осетљиви подаци и лиценцирани софтвери обрисали пре расходовања или поновног коришћења.

Безбедност опреме корисника без надзора

Члан 37.

Корисници система *BISTrezor* треба да осигурају да опрема и софтвер, када су без надзора, имају одговарајућу заштиту, ради онемогућавања приступа заштићеним информацијама и подацима.

Остављање осетљивих и поверљивих докумената и материјала

Члан 38.

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

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 39.

Ради 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 *BISTrezor*, 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.

Секретаријат усваја процедуре које садрже инструкције за детаљно извршење послова у оквиру Сектора.

Управљање расположивим капацитетима

Члан 40.

Коришћење ресурса се 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.

Раздвајање окружења за развој, испитивање и рад

Члан 41.

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

За обезбеђивање исправног и безбедног функционисања средстава за обраду података и примену радних процедура задужен је руководилац Сектора.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 42.

Управа за заједничке послове покрајинских органа задужена је за заштиту опреме и софтвера од злонамерних напада који имају намеру да отежају рад или оштете неки умрежен или неумрежен рачунар.

Запослени у Сектору и други корисници мреже, путем које функционише систем *BISTrezor*, дужни су да сваку информацију о нарушавању безбедности пријаве на следећи имејл informaciona.bezbednost@vojvodina.gov.rs у складу са актима којима је ову област регулисала Управа за заједничке послове покрајинских органа.

Поступак контроле и предузимање мера против злонамерног софтвера

Члан 43.

Сектор одређује и примењује контроле откривања, спречавања и опоравка система *BISTrezor*, ради заштите од злонамерног софтвера.

У случају да корисник система *BISTrezor* примети необично понашање рачунара, односно неправилности у раду система *BISTrezor*, запажање треба без одлагања да пријави на следећи имејл cert.bistrezor@vojvodina.gov.rs

Заштита од губитка података

Члан 44.

Сектор израђује резервне копије које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система *BISTrezor*, у случају наступања последица изазваних ванредним околностима у складу с процедуром „*Backup* података система BISTrezor".

Резервне копије информација и података

Члан 45.

Резервне копије информација, софтвера и дупликати система *BISTrezor* редовно се 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 система *BISTrezor*, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија апликација, као и изворни кодови и базе података система *BISTrezor*.

Заштитне копије омогућавају брзо и ефикасно враћање у функцију система *BISTrezor* у случају нежељених догађаја и треба их правити у време када се не умањује расположивост сервиса, апликација и база података.

За чување заштитних копија користе се екстерни и интерни хардискови и *USB* (*Iron key*), Сектор 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, конфигурационих фајлова, апликација, сервиса и база података;
- води евиденцију урађених резервних копија;
- одлаже копије на безбедно место;
- тестира исправност резервних копија и процедуре за прављење заштитних копија;
- рестаурира податке с резервних копија.

За заштиту од губитка података одговоран је роководилац Сектора.

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

Члан 46.

У систему BISTrezor формирају се се записи о догађајима (логови) у вези са активностима корисника и са информационом безбедношћу.

Записивање догађаја

Члан 47.

Сектор прави записе о догађајима и бележи активности корисника система *BISTrezor*, грешке и догађаје у вези с безбедношћу информација, који се морају чувати и редовно преиспитивати.

Записи о догађајима садрже:

- идентификаторе корисника система *BISTrezor*;
- датуме, време и детаље кључних догађаја (нпр. пријављивања и одјављивања);
- идентитет рачунара;
- записе о успешним и одбијеним покушајима приступа систему;
- мрежне адресе.

Заштита информација у записима

Члан 48.

Средства за записивање и записане информације заштићени су 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 49.

Администратори система *BISTrezor* могу да управљају записима на опреми за обраду информација које су под њиховом директном контролом. Активности администратора и оператора система се записују, а записи штите и редовно преиспитују.

Сатови свих одговарајућих система за обраду информација заштите морају бити синхронизовани по гриничком средњем времену.

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

Заштита од злоупотребе техничких безбедносних слабости система *BISTrezor*

Члан 50.

Интерни ЦЕРТ анализира систем *BISTrezor* и утврђује степен изложености система *BISTrezor* потенцијалним безбедносним слабостима, те предузима одговарајуће мере у погледу уклањања препознатих слабости и примену мера заштите.

Управљање техничким рањивостима

Члан 51.

Интерни ЦЕРТ благовремено прикупља информације о техничким рањивостима информационог система *BISTrezor*, вреднује изложеност тим рањивостима и предузима одговарајуће мере, имајући у виду припадајуће ризике.

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.

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, Интерни ЦЕРТ је дужан да одмах предложи подешавања или инсталацију додатног софтвера који ће отклонити уочене рањивости. Прво се узимају у разматрање системи с високим ризиком.

Ограничења у погледу инсталације софтвера

Члан 52.

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености система *BISTrezor* безбедносним слабостима.

Процедуром „Инсталација *outsource* програма (комерцијалних програма)" детаљније је дефинисано које врсте софтвера администратор сме да инсталира, а које су забрањене у смислу безбедности система *BISTrezor*.

Обезбеђивање да активности на ревизији система *BISTrezor* имају што мањи утицај на функционисање система

Члан 53.

Приликом спровођења ревизије система *BISTrezor*, Сектор обезбеђује да ревизија има што мањи утицај на фукционисање система *BISTrezor*.

Ревизију ИКТ система може да планира само Интерни ЦЕРТ, заједно с руководиоцем Сектора и начелником Одељења.

Заштита података у комуникационим мрежама, укључујући уређаје и водове

Члан 54.

Заштиту података у комуникационим мрежама, уређајима и водовима од неовлашћеног приступа котролише и спроводи Управа за заједничке послове покрајинских органа.

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

Члан 55.

Заштиту података који се преносе комуникационим средствима унутар Секретаријата, као и између Секретаријата и директних буџетских корисника, спроводи Управа за заједничке послове покрајинских органа.

Споразуми о преносу информација из система *BISTrezor*

Члан 56.

Безбедан пренос пословних информација из система *BISTrezor* између Секретаријата и трећег лица обезбеђује се поштовањем споразума о преносу информација.

Споразум о преносу информација треба да садржи:

1) одговорности 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) дефинисање и идентификовање курира;

5) обавезе и одговорности у случају инцидената нарушавања безбедности информација, као што је губитак података;

6) одржавање ланца надзора за информације у току преноса.

Размена електронских порука

Члан 57.

О безбедности и веродостојности електронских порука стара се Управа за заједничке послове покрајинских органа.

Споразуми о поверљивости или неоткривању

Члан 58.

Решењем о одређивању лица за приступ посебно осетљивим подацима и информацијама у систему *BISTrezor* дефинисани су поверљивост и заштита информације о систему *BISTrezor* и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

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

Члан 59.

Обезбеђивање апликативних услуга у јавним мрежама

Управа за заједничке послове покрајинских органа задужена је да обезбеђује мрежу и штити информације обухваћене апликативним услугама, које пролазе кроз јавне мреже, од малверзација, неовлашћеног откривања података и модификовања. Идентитет корисника и овлашћења за рад проверава систем *BISTrezor*.

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

Одговорност појединаца и поступак одговора на инциденте

Члан 60.

Посебним процедурама уређује се начин одговора на инциденте нарушавања безбедности информација система *BISTrezor* и одређује се особа за контакт у случајевима нарушавања безбедности, као и за контакте с Националним ЦЕРТ-ом.

Секретаријат оснива Интерни ЦЕРТ чији је задатак да – заједно са Сектором – придржавајући се процедура, планира, детектује, анализира и да информише надлежне у току и након инцидента.

Интерни ЦЕРТ треба да поседује одговарајућа техничка знања како би на најбржи и одговарајући начин могао да одговори на безбедносне инциденте.

Ради превенције, Интерни ЦЕРТ треба да обезбеди више (различитих и другачијих) механизама за комуникацију и координацију у случају нарушавања безбедности.

У случају било каквог инцидента који може да угрози безбедност ресурса система *BISTrezor*, корисник система *BISTrezor* дужан је да одмах о томе обавести надлежне путем имејла cert.bistrezor@vojvodina.gov.rs

Извештавање о догађајима у вези са безбедношћу информација

Члан 61.

Сви корисници система *BISTrezor* морају бити упознати са обавезом и с процедуром извештавања о догађајима у вези с безбедношћу информација.

Интерни ЦЕРТ дужан је да припреми план за обезбеђење континуитета рада система *BISTrezor*.

Руководилац Сектора даје план на усвајање руководиоцу Секретаријата.

У случају погрешног функционисања или других аномалијских понашања система *BISTrezor*, извештава се исто као и у случају догађаја у вези с безбедношћу информација.

Када је индетификован инцидент, корисник система *BISTrezor* дужан је да одмах обустави рад и да обавести Инертни ЦЕРТ, ради заштите ресурса ИКТ система.

Интерни ЦЕРТ води евиденцију о свим инцидентима, као и о пријавама инцидената, у складу са актима на основу којих се против одговорних лица могу да воде дисциплински, прекршајни или кривични поступци.

Извештавање о утврђеним слабостима система заштите

Члан 62.

Корисници система *BISTrezor* су у обавези да извештавају Интерни ЦЕРТ о уоченим и утврђеним слабостима ИКТ система, у што краћем року, како би се спречили инциденти нарушавања безбедности информација, као и настанак штете.

Догађаји у вези с безбедношћу информација се оцењују и – у складу с тим – доноси се одлука да ли је потребно да се класификују као инциденти нарушавања безбедности информација.

Руководилац Секретаријата ће посебним актом уредити начин поступања чланова Интерног ЦЕРТ-а и запослених у Сектору у случају инцидента у систему *BISTrezor*.

Одговор на инциденте нарушавања безбедности информација

Члан 63.

Секретаријат је у обавези да усвоји план за обезбеђење континуитета рада система *BISTrezor*.

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

Прикупљање доказа

Члан 64.

На предлог Сектора, Секретаријат дефинише и примењује процедуре за идентификацију, сакупљање и чување информација које могу да служе као доказ у случају спровођења поступка за утврђивање одговорности запослених у Сектору и корисника система *BISTrezor* у случају инцидента којим се нарушавају безбедност и функционисање система *BISTrezor*.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 65.

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

Планирање континуитета мера безбедности информација

Члан 66.

На предлог Сектора, Секретаријат доноси план за обезбеђење континуитета рада система *BISTrezor*.

Имплементација континуитета безбедности информација

Члан 67.

Да би се осигурао потребан ниво континуитета безбедности информација система *BISTrezor* током ванредних ситуација, Интерни ЦЕРТ примењује процедуре и контроле описане у плану за обезбеђење континуитета рада система *BISTrezor*.

Интерни ЦЕРТ редовно врши проверу усвојених процедура контроле континуитета безбедности информација система *BISTrezor*, како би оне биле важеће 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 врсте и броја сервера и типа базе података, процеса, процедуре и контроле безбедности информација.

Поступање са информацијама

Члан 68.

Корисник система *BISTrezor* не може захтевати приступ информацијама које му нису потребне за обављање послова, а информације које су му доступне дужан је да користи на прописани начин.

Корисник система *BISTrezor* не сме да неовлашћено саопштава информације до којих је дошао у обављању својих послова.

При обављању приватних послова, корисник система *BISTrezor* не сме да користи информације из система *BISTrezor*, које су му службено доступне ради стицања погодности за себе или с њим повезана лица.

Заштита приватности

Члан 69.

Ради заштите приватности, корисник система *BISTrezor* не сме да износи личне податке из евиденција које се у систему *BISTrezor* воде о другом запосленом, осим у законом предвиђеним случајевима.

III. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза Секретаријата

Члан 70.

Обавеза Сектора јесте да најмање једном годишње спроведе проверу безбедности система *BISTrezor*.

Провера може да се спроведе самостално или уз ангажовање спољних експерата. Провером се оцењују адекватност нивоа информационе безбедности путем провере мера заштите, процедура и одговорности утврђених овим правилником.

Сектор је дужан да састави извештај о извршеној провери и да га достави руководиоцу Секретаријата. На основу извештаја, Сектор може руководиоцу Секретаријата да дâ предлог о измени овог правилника.

Ступање на снагу Правилника

Члан 71.

Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном листу АП Војводине".

ПОКРАЈИНСКИ СЕКРЕТАРИЈАТ ЗА ФИНАНСИЈЕ

Број: 102-011-12/2020-02

Дана: 15. март 2021. године

ПОКРАЈИНСКА СЕКРЕТАРКА ЗА ФИНАНСИЈЕ

СМИЉКА ЈОВАНОВИЋ

С. Јовановић