Република Србија
МИНИСТАРСТВО ТУРИЗМА И
ОМЛАДИНЕ
Број: 001122358 2024 13450 002
003 020 092
Датум: 25.03.2024
Немањина 22-26
Београд

На основу члана 44. Закона о државној управи („Службени гласник РС" бр. 79/05, 101/07, 95/10, 99/14,47/18 и 30/18), а у вези члана 8. Закона о информационој безбедности („Службени гласник РС", бр. 6/16 и 94/17 и 77/19) и члана 2. 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 („Сл. гласник РС", број 94/16-21) министар доноси:

ДИРЕКТИВУ
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО - КОМУНИКАЦИОНОГ СИСТЕМА МИНИСТАРСТВА ТУРИЗМА И ОМЛАДИНЕ

I Уводне одребе

Члан 1.

Овом директивом, у складу са Законом о информационој безбедности и Уредбом 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, утврђују се мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система Министарства туризма и омладине (у даљем тексту: МТО).

Акт о безбедности ИКТ система позива се на друга документа (поступке и упутства), који су саставни део овог акта, а којима се ближе одређују поједини процеси и активности заштите безбедности ИКТ система.

Циљеви Директиве о безбедности

Члан 2

Циљеви доношења Директиве о безбедности су:

1) одређивање начина и процедуре за постизање и одржавање адекватног нивоа безбедности ИКТ система;
2) спречавање и ублажавање последица инцидената којима се угрожава или нарушава информациона безбедност;
3) подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4) додељивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
5) свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Члан 3.

Мере прописане овом директивом се односе на све организационе јединице МТО, на све запослене - кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе МТО.

Непоштовање одредби ове директиве повлачи дисциплинску одговорност запосленог-корисника информатичких ресурса МТО сходно ***Поступку управљања људским ресурсима са аспекта безбедности ИКТ система (ISMS.03).***

За праћење примене ове директиве обавезују се сви руководиоци појединих организационих целина МТО, а за управљање програмима провера ИКТ система делегира се одговорност лицу које је овлашћено од стране министра Решењем.

Поједини термини ИКТ система
Члан 4

Поједини термини у смислу ове директиве дати су у оквиру члана 2. Закона о информационој безбедности („Службени гласник РС", број 6/16, 94/17, 77/19), као и у односним документима на које се позива овај Акт.

Термини, који се користе у функционисању ИКТ система, 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 воде, чувају*, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, 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) оператор ИКТ система је правно лице, орган власти или организациона јединица органа власти* који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;
3) 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;
4) тајност је својство које значи да податак није доступан неовлашћеним лицима;
5) интегритет значи очуваност изворног садржаја и комплетности податка;
6) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
7) 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;
8) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
9) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
10) 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;
11) инцидент је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система; *
11а) јединствени систем за пријем обавештења о инцидентима је информациони систем у који се уносе подаци о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности; *
12) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
13) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
14) ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
15) орган власти је државни орган, орган аутономне покрајине, орган јединице локалне самоуправе, организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења; *
16) служба безбедности је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије;
17) самостални оператори ИКТ система су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове и службе безбедности;
18) компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
19) криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
20) криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
21) криптографски производ је софтвер или уређај путем кога се врши криптозаштита;
22) криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
23) безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
24) информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично; *
25) услуга информационог друштва је услуга у смислу закона којим се уређује електронска трговина; *
26) пружалац услуге информационог друштва је правно лице које је пружалац услуге у смислу закона којим се уређује електронска трговина. *

*Службени гласник РС, број 77/2019

II Мере заштите

Члан 5.

Приликом планирања и примене мера заштите ИКТ система МТО-а неопходно је применити следећа начела:

1) ***начело управљања ризиком*** — избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности;
2) ***начело свеобухватне заштите*** — мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система;
3) ***начело стручности и добре праксе*** — мере се примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности;
4) ***начело свести и оспособљености*** - сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесна ризика и поседују одговарајућа знања и вештине.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Мере заштите подељене су по односним областима и то:

1. Организациона структура, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу

Сваки запослени-корисник ресурса ИКТ система је одговоран за безбедност ресурса ИКТ система које користи ради обављања послова за које је задужен.

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите и безбедности ИКТ система, као и за обављање послова из области безбедности целокупног ИКТ система одговоран је непосредни руководилац организационе јединице којој запослени припада у складу са важећом систематизацијом радних места МТО.

Под пословима из области безбедности утврђују се:

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

Ближе дефинисање одговорности запослених, којима се остварује управљање информационом безбедношћу, остварује се у односним процедурама и политикама система менаџмента безбедношу информација и посебним актима министра МТО којима се именују одговорна лица за послове из области безбедности ИКТ система, а који се односе на:

- Предлагање нацрта основних докумената у вези безбедности ИКТ система нпр., политика безбедности ИКТ система, политика класификовања података, политика контроле приступа, прихватљива употреба ресурса, методологија оцене и поступања са ризиком, итд.;
- Координацију процеса процене ризика;
- Предлагање мера заштите безбедности ИКТ система;
- Контакт са специјалним заинтересованим групама;
- Припрему плана обука или упуства у вези безбедности ИКТ система;
- Предлагања циљева безбедности ИКТ система;
- Извештавање о резултатима предузетих мера;
- Предлагање унапређења и корективних мера у области безбедности ИКТ система;
- Предлагање буџета и других неопходних ресурса за заштиту информација;
- Обавештавање највишег руководства о значајним ризицима;
- Извештавање о предузетим мерама заштите;
- Саветовања највишег руководства о свим питањима у вези безбедности ИКТ система;
- Координацију активностима одговора на безбедносне инциденте;
- Преиспитивање и ажурирање докумената у вези безбедности ИКТ система;
- Спровођење обука запослених у вези методологије за процену ризика;
- Спровођење раздвајања конфликтних дужности и подручја одговорности;
- Спровођење активности у вези стварања свести о значају безбедности ИКТ система;
- Спровођење обука у вези безбедности ИКТ система за новозапослене;
- Спровођење интерне контроле сопствених ИКТ система (проверу усклађености примењених мера ИКТ система са Актом о безбедности ИКТ система и планираним поставкама);
- Верификовање да су корективе мере отклониле узрок неусаглашености;
- Спровођење оцене ризика за екстерно набављене активности (outsource);
- Координацију процеса анализе ризика и припреме плана за одговор у вези континуитета пословања;
- Идентификовање информационих добара и одговорности за њихову заштиту;
- Одржавање листе свих значајних информатичких ресурса;
- Спровођење расходовања опреме која више није у употреби на безбедан начин;
- Спровођење процене поузданости потенцијалних кандидата — outsource партнера којима се поверавају активности у вези са ИКТ системом;
- Примање информација у вези безбедносних инцидената и припремања евиденције за надлежне органе у вези инцидената;
- Анализирање безбедносних инцидената како би се спречило њихово понављање;
- Одобравање одговарајућих метода за заштиту мобилних уређаја, мреже и других комуникационих канала;
- Предлагање метода аутентификације, политике password-а, метода енкрипције, итд.;
- Предлагање правила за безбедан рад са удљености (teleworking).
- Дефинисање неопходне безбедносне поставке за Интернет сервисе;
- Предлагање принципа за безбедан развој информационих система;
- Преиспитивање записа (log-ова) активности корисника како би се препознала сумњива понашања.

Да би се смањиле прилике за неовлашћену или ненамерну модификацију или злоупотребу имовине организације, раздвојене су конфликтне дужности и подручја одговорности на основу процене ризика по безбедност ИКТ система и дефинисаних принципа раздвајања. Процена ризика по безбедност ИКТ система спроводи се на начин дефинисан у **Поступку управљања ризицима по безбедност ИКТ система (ISMS.01) и Упутству за оцењивање ризика по безбедност ИКТ система (ISMS.13).**

2. Безбедност рада на даљину и употреба мобилних уређаја

Министарство дозвољава рад на даљину и употребу мобилних уређаја од стране корисника ИКТ система, уколико је осигурана безбедност рада у случају обављања послова ван Министарства, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења, крађе и губитка мобилних уређаја

Запослени-корисници ресурса ИКТ система, регистровани корисници, приступају са удаљених локација на начин дефинисан у **Упутству за безбедно коришћење мобилнних уређаја (ISMS.08).**

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

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

Лица која користе ИКТ систем односно управљају ИКТ системом оспособљавају се за посао који раде и разумеју своју одговорност, кроз примену **Поступка управљања људским ресурсима са аспекта безбедности ИКТ система (ISMS.03).** Приликом увођења новозапослених на радна места и прерасподеле на друга радна места, применом поменутог поступка обезбеђује се потребан ниво свести о ризицима у вези њихових активности у односу на ИКТ система безбедности и у вези садржаја овог Акта и обавезне примене докумената која се односе на њихов рад у оквиру ИКТ система.

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

Сви корисници ИКТ система су дужни да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система министарства и након престанка или промене радног ангажовања. Промена привилегија ће се извршити у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.
У случају престанка радног ангажовања запосленог односно престанка коришћења ИКТ система од стране других корисника, поступа се по утврђеним процедурама:

- **Поступак управљања људским ресурсима са аспекта безбедности ИКТ система (ISMS.03)**
- **Упутство за прикључење на ИКТ систем (ISMS.15).**

5. Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Информациона добра МТО су сви ресурси: информације, хардвер, софтвер, људски ресурси који садрже пословне информације, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, укључујући све папирне и електронске записе, рачунарску и телекомуникациону опрему, опрему за копирање и архивирње, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, људске ресурсе и све остале неоходне ресурсе за несметани рад запоселних у Министарству.

Предмет заштите су:

- хардверске и софтверске компоненте ИКТ система;
- апликације и сервиси Министраства;
- подаци који се обрађују или чувају на компонентама ИКТ система;
- кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система;
- комуникациони линкови

Лице које користи ИКТ систем одговорно је за заштиту информационих добара као и лице које је повезано са релевантним информационим добром сходно **Упутству за коришћење ИКТ система (ISMS.10) и Упутству за коришћење интернета и е-поште (ISMS.12)**, као и важећих уредби које се односе на поступаіье са тајним подацима. Начин идентификовања информационих добара дефинисан је у **Поступку управљања ризицнма по безбедност ИКТ система (ISMS.01).**

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

Начин класификације података и информација дефинисан је у **Поступку управљања ризицима по безбедност ИКТ система (ISMS.01).**

Подаци који се налазе у ИКТ систему представљају тајну ако су тако дефинисани сходно важећем Закону о тајности података и у Каталогу докумената, података и информација који треба да буду означени степеном тајности «Интерно» и «Поверљиво» у МТО (бр. 82-00-1/2023-02 од 16.03.2023.) и Каталогу докумената, података и информација који треба да буду означени степеном тајности «Државна тајна» и «Строго поверљиво» у МТО (бр. 82-00-2/2023-02 од 16.03.2023.)

Подаци који се означе као тајни, морају бити заштићени у складу са важећим одредбама:

- Закона о тајности података,
- Закон о слободном приступу информацијама од јавног значаја
- Закон о заштити података о личности
- Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима,
  Уредбе о посебним мерама физичко-техничке заштите тајних података,
- Уредбе о начину и поступку означавња тајности података, односно докумената,
- Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа.

7. Заштита носача података

У МТО је успостаљена организација приступања и рада са подацима сходно **Поступку управљања ризицима по безбедност ИКТ система (ISMS.01).**

Носачи података који се означе као тајни, морају бити заштићени у складу са одредбама Закона о тајности података и односних уредби.

Евиденцију носача на којима су снимљени подаци, води руководилац сектора коме носач података припада и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа сходно **Поступку управљања ризицима по безбедност ИКТ система (ISMS.01)** и Уредби о начину и поступку означавања тајности података, односно докумената.

У случају транспорта медија са подацима поступа се сходно **Упутству за одржавање ИКТ система (ISMS.09).**

У случају истека рокова чувања података који се налазе на медијима, подаци морају

бити неповратно обрисани на начин дефинисан у **Упутству за одржавање ИКТ система (ISMS.09).**

МТО је корисник LAN мрежне инфраструктуре која је у ингеренцији УЗЗПРО-а.

8. Ограничење приступа подацима и средствима за обраду података

Приступ ресурсима ИКТ система одређен је документима **Упутство за прикључење на ИКТ систем (ISMS.15), Упутство за контролу приступа (ISMS.04), Упутство за обезбеђење објекта (ISMS.02) и Упутство за одржавање ИКТ система (ISMS.09)** као и важећим уредбама које се односе на рад са тајним подацима.

Сви запослени МТО-а дужни су да поштују правила безбедног и примереног коришћења ресурса ИКТ система датим **у Упутству за коришћење ИКТ система- општа правила (ISMS.10) и Упутству за коришћење интернета и е-поште (ISMS.12).**

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

Право приступа ИКТ систему МТО-а имају сви корисници ИКТ система који приступају заштићеним ресурсима из пословних разлога.

Они имају имају само један доменски налог којим приступају свим ресурсима који су неопходни за обављање пословних задатака.

Налози могу бити администраторски и кориснички.

Корисницима ИКТ система који имају приступ информацијама и опреми за обраду информација, по престанку запослења или истеку уговора, укида се право на приступ ИКТ систему.

У циљу заштите ИКТ система, примењују се строга правила контроле приступа ИКТ систему и његовим деловима, која се у редовним временским интервалима прате од стране одговорних лица. Права приступа и спречавање неовлашћеног приступа ИКТ систему дефинисани су у документима:

- **Упутства за прикључење на ИКТ систем (ISMS.15)**
- **Упутство за контролу приступа (ISMS.04)**, као и у оквиру документа **Упутство за обезбеђење објеката (ISMS.02)**.

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Аутентификација корисника којима је одобрен приступ систему врши се путем корисничког имена и лозинке.

Сви корисници ИКТ система су дужни:

- да привремене шифре промене приликом првог пријављивања;
- да корисничко име и лозинку држе у тајности и не откривају их другим лицима, укључујући и надређене особе;
- да избегавају чување корисничког имена и лозинке у писаном облику;
- да промене лозинку увек када постоји било какав наговештај могућег компромитовања.

Сви корисници ИКТ система обучавају се у погледу сврхе и начина употребе ИКТ система, као и одговорностима која проистичу из тога. Одговорности корисника за заштиту сопствених средстава за аутентикацију утврђена су у **Упутству за коришћење ИКТ система-општа правила (ISMS.10)**.

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

У МТО-у није предвиђена криптозаштита података.

Ради заштите тајности, аутентичности и интегритета података, МТО може да размотри коришћење одговарајућих мера криптозаштите.

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

У оквиру Министарства туризма и омладине НИЈЕ имплементиран систем видео надзора, ни на једној од три локације на којима послује Министарство туризма и омладине. Обзиром да се пословне просторије министарства налазе у оквиру објеката које су у државном власништву и да је министарство "закупац" тих просторија, нема потребе да се министарство бави питањима физичке обезбеђења простора, већ је то на УЗЗПРО и служби безбоедности.

Систем видео надзора није имплементиран у деловима објекта (спратовима) које користи Министарство туризма и омладине.

Систем видео надзора је имплементиран од стране "Управе за заједничке послове републичких органа" на улазима објекта и око објекта. Ова управа такође врши и одржавање система видео надзора.

Министарство туризма и омладине нема директан приступ систему видео надозора и нема податке о техничким карактеристикама видео камера и видео снимача.

Систем контроле приступа

У оквиру ИТ система Министарства туризма и омладине НИЈЕ имплементиран систем за контролу приступа као ни систем за евиденцију уласка/изласка запослених из објеката.

Начин физичке заштите објеката, простора, просторија, односно зона у којима се налазе средства и документи ИКТ система и у којима се обрађују подаци у ИКТ систему дефинисан је **Упутством за обезбеђење објекта (ISMS.02)** и одредбама Уредбе о посебним мерама физичко-техничке заштите тајних података ("Службе ни гласник РС", бр. 97/2011-5).

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

Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности имовине у ИКТ систему дефинисана је **Упутством за обезбеђење објекта (ISMS.02)** и одредбама Уредбе о посебним мерама физичко-техничке заштите тајних података ("Службени гласник РС", бр. 97/2011-5).

Опрема се мора исправно одржавати да би се осигурали њена непрекидна расположивост и интегритет, а на начин описан **Упутством за одржавање ИКТ система (ISMS.09)**. У случају ангажовања трећих лица на одржавању ИКТ система или његових делова, сходно **Упутству за управљање односима са испоручиоцима (ISMS.05),** уговорима се дефинишу обавезе заштите података, док су **Упутством за коришћење ИКТ система (ISMS.10)** дефинисана општа правила којих се морају придржавати сви корисници ИКТ система и његових делова који су у власништву МТО.

Министарство туризма и омладине поседује само један сервер. Министарство нема у свом власништву друге серверске опреме нити уређаја за складиштење података. У оквиру ИТ система Министарства туризма и омладине има један физички сервер сместен у сервер Сали УЗЗПРО. На главној и удаљеним локацијама нема серверске опреме.

У Министарства туризма и омладине нема засебне сервер сале, јер за тим не постоји потреба.

Министарство туризма и омладине користи серверске ресурсе које обезбеђује "Канцеларија за ИТ и еуправу владе Србије - УЗЗПРО" у оквиру државног Дата Центра у Београду. У складу са техничким захтевима Министарства туризма и омладине, канцеларија за ИТ - УЗЗПРО обезбеђује потребне хардверске и софтверске ресурсе за рад апликација.

Сви сервери које "Канцеларија за ИТ - УЗЗПРО" обезбеђује за потребе Министарства туризма и омладине, као и за потребе других министарстава и државних институција, налазе се у државном Дата Центру у Београду.

Дата Центар је "Тиер-3" категорије и спада у ред савремених дата центара са редундантним интернет линковима, редундантним системима за хлађење, редундантим системима напајања, као и модерним системима заштите. Дата центар се налази у Катићевој улици бр 14. у Београду, на 4 и 5 спрату.

"Канцеларија за ИТ - УЗЗПРО" сходно захтевма Министарства туризма и омладине обезбеђује физичке серверске ресурсе или виртуалне серверске ресурсе за рад ИТ апликација у министарству.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду Података

Коришћење ресурса се надгледа, подешава и пројектује у складу са захтеваним капацитетима у наредном периоду, како би се осигурале захтеване перформансе система.

Запослени на пословима ИКТ континуирано надзиру и проверавају функционисање средстава за обраду података и управљају ризицима који могу утицати на безбедност ИКТ система и, у складу са тим, планирају, односно предлажу одговарајуће мере сходно **Поступку управљања ризицима по безбедност ИКТ система (ISMS.01)**.

Исправно и безбедно функционисаіье средстава за обраду података обезбеђује се применом докумената **Упутство за одржавање ИКТ система (ISMS.09)** и **Упутство за заштиту и тестирање ИКТ система (ISMS.17)**.

15. Заштита података и средства за обраду података од злонамерног софтвера

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете ресурсе ИКТ система, као и они који нису неоподни за вршење радних обавеза.

Заштита података и средстава за обраду података од злонамерног софтвера се заснива на превенцији и откривању злонамерног софтвера, отклањању штете, као и на одговарајућим контролама приступа систему и управљања захтеваним и потребним променама.

Имајући у виду навдено Заштита од злонамерног софтвера на мрежи спроводи се на начин описан у **Упутству за одржавање ИКТ система (ISMS.09)**, док су остали корисници обавезни да се придржавају **Упутства за коришћење интернета и електронске поште (ISMS.12)** и **Упутства за коришћење ИКТ система-општа правила (ISMS.10)**, којима се између осталог дефинишу мере заштите од злонамерног софтвера.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави надлежној организационој јединици

16. Заштита од губитка података

Заштита од губитка података у МТО-у врши се израдом резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупног система у случају наступања последица изазваних ванредним околностима.

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

У складу са класификацијом информација по важности МТО примењује мере израде резервних копија, са јасно дефинисаном динамиком израде, начином чувања и тестирања резервних копија.

Детаљне мере у циљу заштите од губитка података прописане су **Упутством за поступање са резервним копијама (ISMS.11)**.

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

У ИКТ систему МТО-а формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу информација, који се морају чувати и редовно преиспитивати.

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

Мере које се предузимају у циљу заштите података о догађајима који могу бити од значаја за безбедност ИКТ система, ближе су уређене **Упутством за одржавање ИКТ система (ISMS.09)** и **Поступком управљања безбедносним инцидентима (ISMS.06)**.

МТО примењује мере заштите ИКТ система и тестирања истих у циљу анализе адекватности и могућности за унапређење, применом мера прописаних **Упутством за заштиту и тестирање ИКТ система (ISMS.17)**. Подаци који проистичу из примене ових мера подлежу обавезама заштите, дефинисаним у **Упутству за поступање са резервним копијама (ISMS.11)**.

18. Обезбеђивање интегритета софтвера и оперативних система

У ИКТ систему МТО-а може да се инсталира само софтвер одобрен од стране овлашћене службе. МТО спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система.

Инсталацију и подешавање софтвера може да изврши само лице које има овлашћење за то, као и треће лице, у складу са уговором о набавци односно одржавању софтвера.

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

Мере у циљу обезбеђења интегритета софтвера и оперативних система се спроводе на начин описан у **Упутству за одржавање ИКТ система (ISMS.09)**, док су остали корисници обавезни да се придржавају **Упутства за коришћење ИКТ систем-општа правила (ISMS.10)**.

19. Заштита од злоупотребе техничких безбедносних слабости ИКТ система

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

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, неопходно је извршити подешавања, односно инстапирање софтвера који ће отклонити уочене слабости, као и онемогућавање неовлашћеног инсталирања софтвера који може довести до угрожавања безбедности ИКТ система.

Опште мере које се примењују у циљу заштите ИКТ система од злоупотребе техничких слабости, дефинисане су **Упутством за заштиту и тестирање ИКТ система (ISMS.17)**.

20. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утинај на функиионисање система

Ревизија ИКТ система се вршити тако да има што мањи утицај на пословне процесе корисника-запослених, а с тим у вези, примењују се мере дефинисане у **Упутству за заштиту и тестирање ИКТ система (ISMS.17)**.

21. Заштита података у комуникационим мрежама укључујући уређаје и водове

Комуникациона мрежа, укључујући и уређаје и водове обезбеђује се на одговарајући начин како би се онемогућило пресретање, неовлашћено прикључивање и злоупотреба података. Ради заштите података у комуникационим мрежама, уређајима и водовима, врши се њихова контрола и заштита од неовлашћеног приступа. Да би се ово обезбедило примењују се мере дефинисане у Упутству за одржавање ИКТ система (**ISMS.09**), Упутству за прикључење на ИКТ систем (**ISMS.15**), Упутству за обезбеђење објеката (**ISMS.02**) и Упутству за контролу приступа (**ISMS.04**).

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

МТО размену поверљивих података врши искључиво у оквиру LAN мреже, док се за размену података између удаљених локација користи VPN. За постојећу LAN рачунарску мрежу постоји делимична техничка документација али она није у власништву Министарства туризма и омладине. Изградња LAN мрежа и израда техничке документације је у надлежности "Канцеларије за ИТ" у оквиру УЗЗПРО. Употреба електронске поште мора бити у складу са правилима поступка, сигурна и у складу са позитивним прописима и пословном праксом.

Електронска пошта се може користити искључиво за пословне потребе. Сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

Безбедан пренос пословних информација између МТО-а и трећег лица обезбеђује се поштовањем споразума о преносу информација.

Споразуми о поверљивости или неоткривању информација обавезују потписнике да их штите, користе и објављују на одговоран и ауторизован начин.

У циљу адекватне заштите и администрације мреже примењују се мере дефинисане у Упутству за одржавање ИКТ система (ISMS.09).

У циљу додатног обезбеђења преноса података, МТО примењује мере контроле приступа ИКТ систему, укључујући и приступ мрежи на начин описан у **Упутство за прикључење на ИКТ систем (ISMS.15) и Упутству за контролу приступа (ISMS.04)**.

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

У току животног века ИКТ система, спроводе се мере одржавања, надоградње, замене и унапређења система и његових делова, при чему се током наведених активности предузимају додатне мера заштите података на начин прописан **Упутством за одржавање ИКТ система (ISMS.09) и Упутством за заштиту и тестирање ИКТ система (ISMS.17)**. Када наведене активности у деловима или у целости изводе трећа лица, примењују се додатне мере заштите утврђене **Упутством за управљање односима са испоручиоцима (ISMS.05)**.

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

МТО у редовним временским интервалима врши тестирање ИКТ система и његових делова у циљу анализе адекватности система заштите и утврђивања могућности за унапређење. Приликом тестирања примењују се све неопходне мере за очување података који се користе током тестирања на начин утврђен **Упутством за заштиту и тестирање ИКТ**

25. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Трећа лица која сходно уговореним одредбама пружају услуге МТО, током чега долазе у додир са ИКТ системом и његовим деловима, имају ограничен приступ истим, у складу са **Упутством за прикључење на ИКТ свстем (ISMS.15)**, и обавезни су да поштују правила и процедуре која се утврђују на начин описан у **Упутству за управљање односима са испоручиоцима (ISMS.05).**

У циљу спречавања неовлашћеног приступа ИКТ систему од стране трећег лица додатно се примењују мере заштите утврђене **Упутством за заштиту и тестирање ИКТ система (ISMS.17)**

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

МТО нема склопљен уговор са трећим лицима за пружање услуга информационе безбедности.

Одржавање уколико дође до уговореног нивоа информационе безбедности и пружених услуга у складу су са условима који су уговорени са пружаоцем услуга, обезбеђује се применом **Упутства за управљање односнма са испоручиоцима (ISMS.05)**.

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

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, сваки корисник ИКТ система је дужан да одмах обавести надлежног руководиоца ИКТ система и предузме мере ради заштите ресурса ИКТ система и спречавања настанка штете.

Надлежно – овлашћено лице води евиденцију о свим инцидентима, као и пријавама инцидената, на основу којих се против корисника ИКТ система који је изазвао инцидент, може водити дисциплински, прекршајни или кривични поступак.

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

Уколико је реч о инциденту који је дефинисан Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, МТО је дужан да обавештење о инциденту достави министарству надлежном за информациону безбедност, Народној банци Србије и регулаторном телу за електронске комуникације.

У случају инцидента који може да угрози безбедност ИКТ система, предузимају се мере дефинисане Поступком управљања безбедносним инцидентима (**ISMS.06**).

Како би након оваквих ситуација, ИКТ систем наставио са нормалним функционисањем, неопходно је спровести мере у циљу опоравка целокупног система или његових делова, које су ближе уређене Упутством за опоравак ИКТ система (**ISMS.14).**

28. Мере које обезбеђују континуитет обављања посла у ванредним околностима

У случају ванредних околности предузимају се мере утврђене планом реаговања у ванредним и кризним ситуацијама. Начин дефинисања мера које обезбеђују континуитет обављања посла у ванредним околностима дефинисан је у **Поступку дефинисања плана континуитета рада (ISMS.07)**, док су неке од мера за реаговање у случају настанка инцидената дефинисане **Упутством за опоравак ИКТ система (ISMS.14)**.

29. Комункациони линкови који су у употреби МТО

Целокупну мрежну инфраструктуру у оквиру Министарства туризма и омладине обезбеђује "Канцеларија за ИТ и еУправу, УЗЗПРО "

30. Ингеренције система који нису у власништву МТО

Одржавање целокупне активне ЛАН опреме у Министарства туризма и омладине је у надлежности УЗЗПРО.Сервери база података и апликативни сервери се бекапују у оквиру процедура за бекап, апроцес бекапа обавља „Управа за заједничке послове републичких органа"Одржавање и администрација серверских апликација за потребе Министарства туризма и омладине врши УЗЗПРО.

У оквиру ИТ система министарства користи се интегрисано Windows антивирус софтверско решење " Windows Defender ". Заштита сервера од вируса и malware-а је у надлежности УЗЗПРО. Министарство туризма и омладине ће у наредном преиоду анлизирати потребу Министартва за куповину сложенојег и сврсиходнијег антивирус програма, а у циљу заштите ИКТ окружења.

У оквиру ИТ система Министарства туризма и омладине користи се интерни Емаил сервер хостован на cloud платформи коју одржава УЗЗПРО.

Министарство туризма и омладине није власник објекта и просторија у коме су смештене службе министарства. Постојећа инфраструктура и опрема у оквиру система за видео надзор је под ингеренцијом канцеларије за ИТ УЗЗПРО и правних субјеката који су власници објекта. Послови физичко техничке заштите су под ингеренцијом МУП-А, а систем видео надзора се користи на улазима излазима из објекта и на простору око објекта

III. ИЗМЕНА ДИРЕКТИВЕ О БЕЗБЕДНОСТИ

У случају настанка промена које могу наступити услед техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, извршиће се потребне измене ове Директиве о безбедности, а с циљем његовог унапређења

IV. ПРОВЕРА ИКТ СИСТЕМА

Обавеза МТО-а је да врши проверу ИКТ система најмање једном годишње ради провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности, усклађених са Директивом о безбедности, мерама заштите прописаним, а складу са Законом о информационој безбедности и Уредбом о мерама заштите, о чему ће се сачинити посебан извештај.

V. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Ова Директива о безбедности ступа на снагу наредног дана од дана његовог објављивања на огласној табли Министратва туризма и омладине.

МИНИСТАР

Хусеин Мемић