На основу члана 8. Закона о информационој безбедности ("Сл. гласник РС", бр. 6/2016 и 94/2017) 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-комуникационог система од посебног значаја ("Сл. гласник РС", бр. 94/2016), в.д. директор Позоришта је дана 29.08.2022. године донео:

ПРАВИЛНИК О УПРАВЉАЊУ ИНФОРМАЦИЈАМА (ПОДАЦИМА) И БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА МАЛОГ ПОЗОРИШТА „ДУШКО РАДОВИЋ"

Уводне одредбе

Члан 1.

Овим правилником, 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-комуникационог система од посебног значаја, утврђују се мере заштите, принципи, начин и процедуре у вези са безбедношћу и ресурсима информационо-комуникационих система Малог позоришта „Душко Радовић" (у даљем тексту: Позориште).

Члан 2.

Мере прописане овим правилником се односе на све организационе јединице Позоришта на све запослене – кориснике информатичких ресурса, као и на трећа лица која користе информатичке ресурсе Позоришта.

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

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

- Информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата:
  - електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
  - 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;
  - податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) овог члана, а у сврху њиховог рада, употребе, заштите или одржавања;
  - организациону структуру путем које се управља ИКТ системом;

- 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;
- Тајност је својство које значи да податак није доступан неовлашћеним лицима;
- Интегритет значи очуваност изворног садржаја и комплетности податка;
- Расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
- 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;
- Непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
- Ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
- 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;
- Инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
- Мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;
- Тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;
- ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;
- Компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;
- Криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;
- Криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
- Криптографски производ је софтвер или уређај путем кога се врши криптозаштита;
- Криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;
- Безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;
- Информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;
- ВПН (Виртуелна приватна мрежа) је „приватна" комуникациона мрежа која омогућава корисницима на раздвојеним локацијама да преко јавне мреже једноставно одржавају заштићену комуникацију;

- MAC адреса (Media Access Control Adress) је јединствен број, којим се врши идентификација уређаја на мрежи;
- BackUp је резервна копија података;
- Download је трансфер података са централног рачунара или web презентације на локални рачунар;
- UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричном енергијом;
- Freeware је бесплатан софтвер;
- Opensource softver отвореног кода;
- Firewall је „заштитни зид" односно систем преко кога се врши надзор и контролише проток информација између локалне мреже и интернета у циљу онемогућавања злонамерних активности;
- USB или флеш меморија је спољашњи медијум за складиштење података;
- CD-ROM (Compact disc – Read only memory) се користи као медијум за снимање података;
- DVD је оптички диск високог капацитета који се користи као медијум за складиштење података;
- Информација је корисни податак који може да утиче на нечије одлуке и понашање, има контекст.

Мере заштите

Члан 4.

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

Члан 5.

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

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 Позоришта надлежни су ангажовани информатичари, у складу са уговором са трећим лицима за пружање услуга информационе безбедности у Позоришту (у даљем тексту: ангажовани информатичари Позоришта).

Кршење безбедносних процедура у ИКТ систему запослени-корисник је дужан да пријави ангажованим информатичарима Позоришта, а они су дужни да предузму одговарајуће мере.

Члан 6.

Под пословима из области безбедности утврђују се:

- послови заштите информационих добара, односно средстава имовине за надзор над пословним процесима од значаја за информациону безбедност,
- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИКТ система Позоришта, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе.

У случају инцидента ангажовани информатичари Позоришта, обавештавају директора Позоришта (у даљем тексту: директор), који у складу са прописима обавештава надлежне органе у циљу решавања.

Управљање информацијама

Члан 7.

Својинска и ауторска права над информацијма (подацима) и софтвером који су креирани коришћењем ИКТ ресурса Позоришта припадају Позоришту.

Директор закључно са руководиоцем службе у којој је информација (податак) креирана, прикупљена или се обрађује је власник податка.

Сви подаци независно од форме у којој се налазе, а Позориште их размењује, чува или обрађује на ИКТ ресурсима, класификују се према степену поверљивости податка.

Запослени који користи класификоване податке одговоран је за поступање са њима и дужан је да их штити у свим фазама коришћења.

Члан 8.

Након што је податак класификован као строго поверљив или поверљив креиран, све непотребне верзије податка, настале током креирања, бришу се са радне станице или се уништава (сецка, цепа) папир на коме је штампана.

Обрада података врши се у сагласности са власником податка и руководиоцима надлежним за област обраде информација.

Подаци у електронској форми класификовани као строго поверљиви или поверљиви чувају се на серверима за чување и размену података у директоријумима са ограниченим правима приступа.

Члан 9.

Слање података класификованих као строго поверљиви или поверљиви одобрава власник података.

Строго поверљиви подаци у електронској форми шаљу се шифровани.

Строго поверљиви или поверљиви подаци пре смештања на преносиви медијум се шифрују.

У случају личног достављања овлашћеном лицу строго поверљивих или поверљивих података на преносивом медијуму, не врши се шифровање.

Члан 10.

Уништавање строго поверљивих или поверљивих података смештених на хард диску врши се коришћењем софтвера за безбедно брисање диска од стране овлашћених лица за информационе технологије.

Уништавање строго поверљивих или поверљивих података смештених на преносивом уређају или медијуму врши се форматирањем уређаја или уништењем уређаја или медијума.

Безбедност рада на даљину и употреба мобилних уређаја

Члан 11.

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.

Запослени-корисници ресурса ИКТ система, могу путем мобилних уређаја, који су у власништву Позоришта и који су подешени од стране ангажованих информатичара Позоришта, да приступају само оним деловима ИКТ система који им омогућавају обављање радних задатака у оквиру њихове надлежности (електронска пошта, здравствени информациони систем и пословни информациони систем), а на основу писане сагласности директора.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ, коришћењем ВПН мреже ИКТ система и листе МАЦ адреса уређаја путем којих је дозвољен приступ, уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Приступ ресурсима ИКТ система Позоришта са удаљених локација, од стране запослених-корисника, у циљу обављања радних задатака, омогућен је путем заштићене ВПН/интернет конекције.

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

Ангажовани информатичари Позоришта, свакодневно контролишу приступ ресурсима ИКТ система и проверавају да ли има приступа са непознатих уређаја (са непознатих МАЦ адреса).

Размена електронске поште

Члан 12.

Размена електронске поште у Позоришту дозвољена је искључиво преко система за размену електронске поште и докумената.

Систем за размену електронске поште не сме да се користи за креирање или дистрибуцију нежељених порука.

Електронске поруке или други електронски подаци, који покушавају да сакрију идентитет пошиљаоца или да представе пошиљаоца као неког другог, нису дозвољени.

Члан 13.

Забрањена је употреба службене адресе електронске поште за размену порука:

- чији је садржај увредљив, клеветнички или застрашујући према било коме, као и поруке које су погрдне за било ког појединца или групу,
- које својим садржајем дискриминишу по било ком основу,
- којима се открива пословна тајна Позоришта или пословног партнера, те лични подаци корисника услуга Позоришта који могу да нанесу штету Позоришту било које врсте,
- које служе за политичку или другу пропаганду,
- које својим садржајем ометају запослене у раду и онемогућавају редовну размену пословних информација (тзв. „ланчане поруке“ и сл.).

Члан 14.

Нежељена пошта се смешта у карантин. Корисник се обавештава о порукама које су смештене у карантин и омогућава му се приступ карантину.

Није дозвољено слање електронских порука без наслова или порука већих од прописане величине. О свакој промени у коришћењу система за размену електронске поште корисник се обавештава електронским путем.

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

Члан 15.

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

Сваки новозапослени-корисник ИКТ ресурса треба да се упозна са одговорностима и правилима коришћења ИКТ ресурса, односно омогућити да сваки новозапослени приликом потписивања уговора о раду потпише да је упознат и са овим правилником.

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

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица корисника ИКТ система

Члан 16.

У случају промене послова, односно надлежности корисника-запосленог, ангажовани информатичари Позоришта ће извршити промену привилегија које је корисник-запослени имао у складу са описом радних задатака, а на основу захтева претпостављеног руководиоца.

У случају престанка радног ангажовања корисника-запосленог, кориснички налог се укида.

О престанку радног односа или радног ангажовања, као и промени радног места, дипломирани правник за правне, кадровске и административне послове, је дужан да обавести ангажоване информатичаре Позоришта, ради укидања, односно измене приступних привилегија тог запосленог-корисника.

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

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 17.

Информациона добра Позоришта су сви ресурси који садрже пословне информације Позоришта, односно, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње правилнике који се односе на ИКТ систем и сл.

Предмет заштите су: хардверске и софтверске компоненте ИКТ система, подаци који се обрађују или чувају на компонентама ИКТ система, кориснички налози и други подаци о корисницима информатичких ресурса ИКТ система.

Заштита носача података

Члан 18.

Ангажовани информатичари Позоришта, ће успоставити организацију приступа и рада са подацима, посебно онима који буду означени степеном службености или тајности у складу са Законом о тајности података, тако да:

- подаци и документи (посебно они са ознаком тајности) могу да се сниме (архивирају, запишу) на серверу на коме се снимају подаци, у фолдеру над којим ће право приступа имати само запослени-корисници којима је то право обезбеђено одлуком начелника и
- подаци и документи (посебно они са ознаком тајности) могу да се сниме на друге носаче (екстерни хард диск, УСБ, ЦД, ДВД) само од стране овлашћених запослених - корисника. Евиденцију носача на којима су снимљени подаци, воде ангажовани информатичари Позоришта и ти медији морају бити прописно обележени и одложени на место на коме ће бити заштићени од неовлашћеног приступа.

У случају транспорта медија са подацима, директор ће одредити одговорну особу и начин транспорта.

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

Ограничење приступа подацима и средствима за обраду података

Члан 19.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју запослени- корисник има.

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

Запослени - корисник 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.

Запослени-корисник који на било који начин злоупотреби права, односно ресурсе ИКТ система, подлеже кривичној и дисциплинској одговорности.

Запослени-корисник дужан је да поштује и следећа правила безбедног и примереног коришћења ресурса ИКТ система, и то да:

- користи информатичке ресурсе искључиво у пословне сврхе;
- прихвати да су сви подаци који се складиште, преносе или процесирају у оквиру информатичких ресурса власништво Позоришта и да могу бити предмет надгледања и прегледања од законом овлашћених лица;
- поступа са поверљивим подацима у складу са законским прописима, а посебно приликом копирања и преноса података;

- безбедно чува своје лозинке, односно да их не одаје другим лицима;
- мења лозинке сагласно утврђеним правилима;
- пре сваког удаљавања од радне станице да се одјави са система, односно закључа радну станицу;
- захтев за инсталацију софтвера или хардвера подноси у писаној форми, одобрен од стране непосредног руководиоца;
- обезбеди сигурност података у складу са важећим прописима;
- приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
- не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
- на радној станици не сме да складишти садржај који не служи у пословне сврхе;
- израђује заштитне копије (бацкуп) података у складу са прописаним процедурама;
- користи интернет и електронску пошту Позоришта у складу са прописаним процедурама;
- прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, ажурирање програма, покретање антивирусног програма и сл.) обављају у утврђено време;
- прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
- прихвати да технике сигурности (анти вирус програми, фирewалл, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;
- не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер.

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

Члан 20.

Право приступа имају само запослени-корисници који имају администраторске или корисничке налоге.

Администраторски налог је јединствени налог којим је омогућен приступ и администрација свих ресурса ИКТ система, као и отварање нових и измена постојећих налога.

Администраторски налог могу да користе ангажовани информатичари и менаџмент.

Кориснички налог се састоји од корисничког имена и лозинке, који се могу укуцавати или читати са медија на коме постоји електронски сертификат, на основу кога/јих се врши аутентификација - провера идентитета и ауторизација - провера права приступа, односно права коришћења ресурса ИКТ система од стране запосленог-корисника.

Кориснички налог додељује администратор, на основу захтева запосленог задуженог за управљање људским ресурсима у сарадњи са непосредним руководиоцем и то тек након уноса података о запосленом у софтвер за управљање људским ресурсима, а у складу са потребама обављања пословних задатака од стране запосленог-корисника.

Администратор води евиденцију о корисничким налозима, проверава њихово коришћење, мења права приступа и укида корисничке налоге на основу захтева надлежног руководиоца.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

Члан 21.

Кориснички налог се састоји од корисничког имена и лозинке.

Лозинка мора да садржи:

- број карактера лозинке мора бити већи од 8
- најмање једно велико слово
- најмање један специјалан знак („#$%&/)
- најмање један број.

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке.

Ако запослени-корисник посумња да је друго лице открило његову лозинку дужан је да исту одмах измени.

Запослени-корисник дужан је да мења лозинку најмање једном у три месеца, а најдуже једном у шест месеци.

Иста лозинка се не сме понављати у временском периоду од годину дана.

Кориснички налог може да се се креира и на основу података који се налазе на медију са квалификованим електронским сертификатом (нпр. лична карта са чипом и уписаним сертификатом).

Неовлашћено уступање корисничког налога другом лицу, подлеже дисциплинској одговорности.

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

Члан 22.

Запослени-корисници користе квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама.

Ангажовани на пословима ИКТ су задужени за инсталацију потребног софтвера и хардвера за коришћење сертификата.

Запослени-корисници су дужни да чувају своје квалификоване електронске сертификате, како не би дошли у посед других лица.

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

Члан 23.

Простор у коме се налазе сервери, мрежна или комуникациона опрема ИКТ система, организује са као административна зона. Административна зона се успоставља за физички приступ ресурсима ИКТ система у контролисаном, видљиво означеном простору, који је обезбеђен механичком бравом. Простор мора да буде обезбеђен од

компромитујућег електромагнетног зрачења (КЕМЗ), пожара и других елементарних непогода, и у њему треба да буде одговарајућа температура (климатизован простор).

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

Члан 24.

Улаз у просторију у којој се налази ИКТ опрема, дозвољен је само администратору ИКТ система / запосленима на пословима ИКТ.

Осим администратора система, приступ административној зони могу имати и трећа лица у циљу инсталације и сервисирања одређених ресурса ИКТ система, а по претходном одобрењу директора, и уз присуство ангажованог информатичара Позоришта.

Просторија мора бити видљиво обележена и у њој се мора налазити противпожарна опрема, која се може користити само у случају пожара у просторији у којој се налази ИКТ опрема и медији са подацима.

Прозори и врата на овој просторији морају увек бити затворени.

Сервери и активна мрежна опрема (свич, модем, роутер, фиревалл), морају стално бити прикључени на уређаје за непрекидно напајање - УПС.

У случају нестанка електричне енергије, у периоду дужем од капацитета УПС-а, овлашћено лице је дужно да искључи опрему у складу са процедурама произвођача опреме.

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

У случају изношења опреме ради селидбе, или сервисирања, неопходно је одобрење директора који ће одредити услове, начин и место изношења опреме.

Ако се опрема износи ради сервисирања, поред одобрења директора, потребно је сачинити записник у коме се наводи назив и тип опреме, серијски број, назив сервисера, име и презиме овлашћеног лица сервисера.

Уговором са сервисером мора бити дефинисана обавеза заштите података који се налазе на медијима који су део ИКТ ресурса Позоришта.

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 25.

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 директору одговарајуће мере.

Пре увођења у рад новог софтвера неопходно је направити копију-архиву постојећих података, у циљу припреме за процедуру враћања на претходну стабилну верзију.

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

У случају да се на новој верзији софтвера који је уведен у оперативни рад примете битни недостаци који могу утицати на рад, потребно је применити процедуру за враћање на претходну стабилну верзију софтвера.

Заштита података и средства за обраду података од злонамерног софтвера

Члан 26.

Заштита од злонамерног софтвера на мрежи спроводи се у циљу заштите од вируса и друге врсте злонамерног кода који у рачунарску мрежу могу доспети интернет конекцијом, имејлом, зараженим преносним медијима (УСБ меморија, ЦД итд.), инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна антивирусних дефиниција.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања преносних медија.

Преносиви медији, пре коришћења, морају бити проверени на присуство вируса. Ако се утврди да преносиви медиј садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером.

Ризик од евентуалног губитка података приликом чишћења медија од вируса сноси доносилац медија.

Директор у договору са руководиоцима организационих јединица одређује који запослени имају право приступа интернету ради прикупљања података и осталих информација везаних за обављање послова у њиховој надлежности.

Корисницима који су прикључени на ИКТ систем је забрањено самостално прикључивање на интернет (прикључивање преко сопственог модема), при чему ангажовани информатичари Позоришта могу да укину приступ интернету у случају доказане злоупотребе истог.

Корисници ИКТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИКТ систем, а сваки рачунар чији се запослени-корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши ангажовани информатичар Позоришта.

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

Корисник ИКТ ресурса дужан је да, одмах пријави непосредном руководиоцу свако уочавање или сумњу о неправилности, или настанку неког инцидента који угрожава рад ИКТ система. Случај се потом пријављује директору.

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

Недозвољена употреба интернета обухвата:

- инсталирање, дистрибуцију, оглашавање, пренос или на други начин чињење доступним „пиратских" или других софтверских производа који нису лиценцирани на одговарајући начин;
- нарушавање сигурности мреже или на други начин онемогућавање пословне интернет комуникације;
- намерно ширење деструктивних и опструктивних програма на интернету (интернет вируси, интернет тројански коњи, интернет црви и друге врсте малициозних софтвера);
- недозвољено коришћење друштвених мрежа и других интернет садржаја које је ограничено;

- преузимање (downлоад) података велике "тежине" које проузрокује "загушење" на мрежи; преузимање (downлоад) материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
- недозвољени приступ садржају, промена садржаја, брисање или прерада садржаја преко интернета.

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

Заштита од губитка података

Члан 27.

Базе података обавезно се архивирају и на преносиве медије (CDROM, DVD, USB, екстерни хард диск), најмање два пута месечно, за потребе обнове базе података.

Базе података се реплицирају на више различитих локација, а једна ван просторија Позоришта.

Остали фајлови-документи се архивирају најмање једном недељно, месечно и годишње.

Сваки примерак годишње копије-архиве чува се у року који је дефинисан Упутством о канцеларијском пословању органа државне управе („Сл. гласник РС", бр. 10/1993, 14/1993-исправка, 67/2016 и 3/2017).

Дневне, недељне и месечне копије-архиве се чувају у просторији која је физички обезбеђена и у складу са мерама заштите од пожара.

Обезбеђивање интегритета софтвера и оперативних система

Члан 28.

У ИКТ систему може да се инсталира само софтвер за који постоји важећа лиценца у власништву Позоришта, односно Фрееваре и Опенсоурце верзије.

Инсталацију и подешавање софтвера могу да врше само ангажовани информатичари Позоришта, односно запослени-корисник који има овлашћење за то.

Инсталацију и подешавање софтвера може да изврши 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.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 29.

Уколико се идентификују слабости које могу да угрозе безбедност ИКТ система, информатичари Позоришта су дужни да одмах изврше подешавање, односно инсталирају софтвер који ће отклонити уочене слабости.

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

Члан 30.

Ревизија ИКТ система се мора вршити тако да има што мањи утицај на пословне процесе корисника- запослених. Уколико то није могуће у радно време, онда се врши након завршетка радног времена корисника-запослених, чији би пословни процес био ометан, уз претходну сагласност директора установе.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 31.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно да се изврши изолација од могућег оштећења.

Мрежна опрема (switch, роутер, firewall) се мора налазити у закључаном рацк орману.

Ангажовани нформатичари Позоришта су дужни да стално врше контролни преглед мрежне опреме и благовремено предузимају мере у циљу отклањања евентуалних неправилности.

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

Члан 32.

Када се пренос података врши између Позоришта и другог лица, могу се закључити споразуми о преносу података и споразуми о поверљивости или неоткривању који садрже одредбе о безбедности преноса података.

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

Члан 33.

Начин инсталирања нових, замена и одржавање постојећих ресурса ИКТ система од стране трећих лица која нису запослена у Позоришту, биће дефинисан уговором који ће бити склопљен са тим лицима.

Ангажовани информатичари Позоришта су задужени за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система ангажовани информатичари Позоришта воде документацију.

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

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

Члан 34.

Приликом тестирања система, подаци који су означени ознаком тајности, односно службености као поверљиви подаци, или су лични подаци, ангажовани информатичари одговарају за податке у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

Заштита средстава ИКТ система која су доступна пружаоцима услуга

Члан 35.

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

Ангажовани информатичари Позоришта су одговорни за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби овог правилника којима су такве активности дефинисане.

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

Члан 36.

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

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

Члан 37.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени-корисник је дужан да одмах обавести ангажоване информатичаре Позоришта.

По пријему пријаве ангажовани информатичари Позоришта су дужни да одмах обавесте директора Позоришта и предузму мере у циљу заштите ресурса ИКТ система.

Уколико се ради о инциденту који је дефинисан у складу са Уредбом о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, („Сл. гласник РС", бр, 94/2016), ангажовани информатичари Позоришта, су дужни да поред директора обавесте и надлежни орган дефинисан овом уредбом.

Ангажовани информатичари Позоришта воде евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 38.

У случају ванредних околности, које могу да доведу до измештања ИКТ система, ангажовани информатичари Позоришта, су дужани да у најкраћем року пренесу делове ИКТ система (или обезбеде функционисање редудантних компоненти на резервној

локацији уколико постоје) неопходне за функционисање у ванредној ситуацији на резервну локацију, у складу са планом реаговања у ванредним и кризним ситуацијама.

Делове ИКТ система који нису неопходни за функционисање у ванредним ситуацијама, складиште се на резервну локацију, коју одреди директор. Складиштење делова ИКТ система који нису неопходни, се врши тако да опрема буде безбедна и обележена, у складу са евиденцијом која се о њој води.

Измена Правилника о безбедности

Члан 39.

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, ангажовани информатичари Позоришта су дужни да обавесте директора, како би он могао да приступи измени овог правилника, у циљу унапређења мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу ИКТ система.

Провера ИКТ система

Члан 40.

Проверу ИКТ система врше ангажовани информатичари Позоришта.

О извршеној провери сачињава се извештај, који се доставља директору на увид.

Прелазне и завршне одредбе

Члан 41.

Овај правилник објављује се на огласној табли и на веб презентацији Позоришта.

Овај правилник ступа на снагу осам дана од дана објављивања на огласној табли Позоришта.

ВД Директор
Малог позоришта „Душко Радовић“

МАЛО ПОЗОРИШТЕ "ДУШКО РАДОВИЋ" * БЕОГРАД