На основу члана 8. Закона о информационој безбедности ("Службени гласник РС", број 6/2016, 94/2017 и 77/2019), чланова 1-8 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 гланик РС", број 94/2016) и члана 46. Статута Позоришта Пуж, Управни одбор је на седници одржаној дана 31.08.2022. године донео

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА У ПОЗОРИШТУ ПУЖ

ОПШТЕ ОДРЕДБЕ

Члан 1.

Овим Правилником ближе се дефинишу мере заштите информационо-комуникационих система у Позоришту Пуж (у даљем тексту: Позориште), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и дужности и одговорности корисника информатичких ресурса у Позоришту.

Термини изражени у овом Правилнику у граматичком мушком роду подразумевају природни мушки и женски род лица на које се односе.

ЦИЉЕВИ

Члан 2.

Циљеви доношења овог акта су :

1) допринос подизању опште свести о ризицима и опасностима који су везани за коришћење информационих технологија;
2) минимизација безбедносних инцидената;
3) допринос развоју одговарајућих безбедносних апликација и обезбеђивање конзистенте контроле свих компонената информационо – комуникационог система (у даљем тексту: ИКТ систем).

ОБАВЕЗНОСТ

Члан 3.

Примена мера заштите ИКТ система, које су прописане овим Правилником, обавезујућа је за све запослене у Позоришту.

За праћење примене одредаба овог Правилника надлежни су директор Позоришта и лице које овласти директор Позоришта (у даљем тексту: Овлашћено лице).

ПОЈМОВИ

Члан 4.

Поједини термини у смислу овог Правилника имају следеће значење:

1) *информационо комуникациони систем* (ИКТ систем) је технолошко организациона целина која обухвата све уређаје за електронску обраду података (хардверске и софтверске компоненте, мрежу и мрежне ресурсе, сервер и осталу комуникациону опрему);

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;

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) *информациона добра* обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично;

МЕРЕ ЗАШТИТЕ

Члан 5.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

ИНФОРМАТИЧКИ РЕСУРСИ ПОЗОРИШТА

Члан 6.

Информатички ресурси Позоришта су сви ресурси који садрже пословне информације Позоришта у електронском облику, или служе за приступ корисника ИКТ систему, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације и слично.

ПРЕДМЕТ ЗАШТИТЕ

Члан 7.

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

КОРИСНИК ИНФОРМАТИЧКИХ РЕСУРСА

Члан 8.

Корисник информатичких ресурса (у даљем тексту: Корисник) јесте постављено лице, запослено лице на одређено или неодређено време, лице ангажовано по основу уговора, консултант или друго радно ангажовано лице коме је одобрен приступ неком информатичком ресурсу Позоришта.

Корисник је одговоран за правилну употребу, тачност и сигурност података приликом коришћења информатичких ресурса Позоришта, односно, лично је одговоран за остваривање својстава података у ИКТ систему Позоришта.

Корисник нема имовинска права над информатичким ресурсима Позоришта.

ДУЖНОСТИ КОРИСНИКА

Члан 9.

Корисник не сме спроводити активности које могу умањити или нарушити сигурност, поузданост или нормално функционисање ИКТ система Позоришта.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне сврхе, а Позориште задржава право да информатичке ресурсе повуче у било ком тренутку и у потпуности задржи све податке, без обавезе да их накнадно преда кориснику.

Корисник непреносиве радне станице је дужан да пословне податке смешта на одређене мрежне дискове на серверу Позоришта.

Изузетно од става 3. овог члана, због потребе посла, подаци се могу привремено сместити на локални диск непреносиве радне станице, ако се са тим сагласи директор Позоришта.

Корисник, као и лица која су задужена за израду резервних копија, дужни су да дневно израђују резервне копије података са мрежних дискова Позоришта.

Корисник дужан је да поштује следећа правила безбедног и примереног коришћења информатичких ресурса и то да:

1) користи информатичке ресурсе искључиво у пословне сврхе;

2) 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 овлашћених лица(министарства и других овлашћених служби);
3) поступа са поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4) безбедно чува своје лозинке, односно, да их не одаје другим лицима;
5) пре сваког удаљавања од радне станице одјави се са система („log out“);
6) користи DVDRW, CDRW и USB екстерне меморије на радној станици само уз одобрење директора Позоришта, а на основу образложеног предлога корисника;
7) захтев за инсталацију софтвера или хардвера подноси у писаној форми (захтев се подноси директору Позоришта);
8) обезбеди сигурност података у складу са важећим прописима;
9) приступа информатичким ресурсима само на основу експлицитно додељених корисничких права/нивоа компетенције;
10) не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
11) не сме да на радној станици складишти садржај који не служи у пословне сврхе;
12) израђује заштитне копије (backup) података, у складу са прописаним процедурама;
13) користи Internet и Internet e-mail сервис у Позоришту у складу са прописаним процедурама;
14) прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, upgrade firmware, покретање антивирусног програма и сл.) обављају у утврђено време;
15) прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
16) прихвати да технике сигурности (антивирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалне претње ИКТ систему;
17) не сме да инсталира, модификује, искључује из рада или брише заштитни, системски или апликативни софтвер;
18) се уздржи од активности којима се изазива неоправдано оптерећење информатичких ресурса Позоришта, као и повећано ангажовање особља на одржавању тих ресурса;
19) не сме неовлашћено да објављује или преноси личне податке до којих је дошао коришћењем информатичких ресурса Позоришта, као што су лозинке, бројеви платних картица, приватни телефонски бројеви и слично и да тиме повреди приватност појединаца;
20) се уздржи од неуобичајено и неоправдано великог коришћења информатичких ресурса Позоришта, а посебно у приватне сврхе.

БЕЗБЕДНОСНИ ПРОФИЛ КОРИСНИКА ИНФОРМАТИЧКИХ РЕСУРСА

Члан 10.

У зависности од описа задатака, послова радног места на које је распоређен и нивоа компетенције, Корисник, на предлог директора Позоришта, стиче одређена права приступа ИКТ систему Позоришта.

Администраторска овлашћења могу добити само лица која су задужена за одржавање информатичких ресурса у Позоришту, уз претходну сагласност директора Позоришта.

КРЕИРАЊЕ ЛОЗИНКЕ

Члан 11.

Лозинка мора да садржи минимум осам карактера, комбинованих од малих и великих слова , цифара и специјалних знакова.

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

Ако Корисник посумња да је друго лице открило његову лозинку, дужан је да се писмено обрати директору Позоришта који ће му дати овлашћење да сам промени лозинку.

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

УПОТРЕБА КОРИСНИЧКОГ НАЛОГА

Члан 12.

Кориснички налог може употребљавати само корисник информатичких ресурса коме је налог издат.

Корисник не сме да омогући другом лицу коришћење његовог корисничког налога, осим директору Позоришта, односно Овлашћеном лицу у случају подешавања радне станице.

Корисник је непосредно одговоран за активности које су реализоване на основу његовог корисничког налога.

Кориснички налози са администраторским овлашћењима користе се само за потребе неопходних интервенција којима се обезбеђује несметан рад информатичких ресурса (у даљем тексту: информатичке интервенције).

УПОТРЕБА АДМИНИСТРАТОРСКОГ НАЛОГА

Члан 13.

Администраторски налози свих пословних апликација, сервера база података и системских апликација за управљање мрежном опремом и уређајима за складиштење података чувају се у затвореним, непровидним ковертама са отиском службеног печата, у обезбеђеном ормару који се закључава и коме има приступ само директор Позоришта или лице које он овласти.

Право коришћења администраторског налога имају само администратори, односно Овлашћена лица за потребе информатичких интервенција.

ПОСТУПЦИ У СЛУЧАЈЕВИМА СИГУРНОСНИХ ИНЦИДЕНАТА

Члан 14.

Корисник је дужан да, без одлагања, директору Позоришта и Овлашћеном лицу пријави инцидент који се десио и свако уочавање или сумњу о наступању инцидената којим се угрожава сигурност ИКТ система.

По пријави инцидента мора се поступати адекватно и ефикасно, а по хитном поступку у случајевима:

1) нарушавања поверљивости информација,
2) откривања вируса или грешака у функционисању апликација,
3) вишеструких покушаја неауторизованог приступа,
4) системских падова и престанка рада сервиса и пада целог сервера.

ЗАШТИТА ОД МАЛИЦИОЗНОГ СОФТВЕРА

Члан 15.

У циљу заштите ИКТ система од малициозног софтвера неопходна је примена:

1) лиценцираног софтвера, односно, забрана коришћења неауторизованог софтвера;
2) правила за заштиту од ризика приликом преузимања фајлова из екстерних извора (података, апликација и сл.).

Приликом преузимања фајлова из става 1. тачка 2) овог члана преносиви медији пре коришћења морају бити проверени на присуство вируса.

Ако се утврди да преносиви медиј садржи вирусе, врше се чишћења медија од вируса, уз сагласност доносиоца медија.

Ризик од евентуалног губитка података, приликом чишћења медија антивирусним софтвером, сноси доносилац медија.

СИГУРНОСТ ЕЛЕКТРОНСКЕ ПОШТЕ

Члан 16.

У циљу сигурности коришћења сервиса електронске поште морају се поштовати следећа правила:

1) електронска пошта са прилозима не сме се отварати ако долази са сумњивих и непознатих адреса, већ се мора избрисати;
2) забрањено је коришћење електронске поште у приватне сврхе, као и коришћење приватних налога електронске поште у пословне сврхе.

ПОСТУПАЊЕ СА ПРЕНОСИВИМ МЕДИЈИМА

Члан 17.

Преносиви медији који садрже податке морају да буду прописно обележени , потписани и чувани на безбедном месту, код Овлашћеног лица.

У случају да је потребно брисање података који се налазе на преносивим медијима, неопходно је обезбедити њихово неповратно брисање.

Уколико се донесе одлука о стављању одређених преносивих медија ван употребе, они тада, приликом стављања ван употребе, морају бити физички уништени.

ФИЗИЧКА СИГУРНОСТ ИНФОРМАТИЧКИХ РЕСУРСА

Члан 18.

У циљу физичке сигурности информатичких ресурса морају се обезбедити следећи услови:

1) сервиси, сторици (storage) и комуникационо чвориште у просторијама Позоришта морају бити смештени у посебној просторији (сервер соби), која испуњава стандарде противпожарне заштите и поседује редудантно напајање електричном струјом и адекватну климатизацију, као и видео надзор, са забраном приступа незапосленим лицима;
2) приступ сервер соби, поред лица која су задужена за одржавање ИКТ система, могу имати и друга лица, уз претходно одобрење директора Позоришта;
3) радна станица мора да буде примерено физички обезбеђена са циљем детекције и онемогућавања физичког приступа или оштећења критичних компонената;
4) просторије у којима се тренутно не борави морају бити обезбеђене од неовлашћеног физичког приступа;

5) штампачи, копир машине и факс машине морају бити лоциране унутар физички безбедне зоне, ради спречавања неовлашћеног копирања и преноса осетљивих информација;
6) медији са поверљивим подацима (USB и екстерни harddiskovi) морају бити заштићени од неауторизованог приступа и прегледа.

ПРИСТУП ИКТ СИСТЕМУ ПОЗОРИШТА

Члан 19.

Приступ свим компонентама ИКТ система мора бити аутентификован.

Овлашћено лице на основу прецизног писаног захтева, додељује Кориснику корисничко име, лозинку и привилегије, као и налог за електронску пошту.

Кориснику се додељују само привилегије које су неопходне за реализацију његових радних обавеза.

У случају престанка радног односа, или радног ангажовања у Позоришту, Кориснику укида се право приступа ИКТ систему.

У случају одсуства са посла у периоду дужем од месец дана (у законом предвиђеним случајевима), Кориснику се привремено укида право приступа ИКТ систему, до повратка на рад.

О престанку радног односа или радног ангажовања, одсуству са посла дужем од месец дана, као и о промени радног места Корисника, самостални финансијско-рачуноводствени сарадник је дужан да обавести директора Позоришта ради укидања, односно, измена приступних привилегија тог Корисника.

Корисник, након престанка радног ангажовања у Позоришта, не сме да открива поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система.

Корисник не може имати удаљени (remote) приступ ИКТ систему. Удаљени приступ може имати искључиво Овлашћено лице.

Трећем лицу се могу одобрити права приступа ИКТ систему уз претходно склапање одговарајућег уговора, којим се прецизно дефинишу услови и обим права приступа, укључујући и све релевантне безбедносне захтеве.

Изузетно од става 8. овог члана, у случају неопходних и хитних послова, могу се одобрити права приступа трећем лицу по усменом налогу директора Позоришта, односно, Овлашћеног лица, о чему ће се накнадно, по завршетку хитног посла, сачинити записник о оствареном приступу.

Ако се установи повреда уговорне обавезе или прекорачење овлашћења по основу уговора, одобрени приступ се одмах укида.

ИНСТАЛАЦИЈА И ОДРЖАВАЊЕ СОФТВЕРА

Члан 20.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужено је Овлашћено лице које је дужно да поступа у складу са прописаним процедурама и упутствима.

Управа Позоришта обезбеђује Кориснику коришћење радне станице (десктоп или лаптоп) са преинсталираним и правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачки програми (драјвери), пословно и развојно окружење, софтвер за антивирусну заштиту, разне помоћне апликације), који је типски за све радне станице и који преставља минимум потребан за обављање стандардних послова радних места у Позоришту.

Овлашћено лице врши оцену конзистентности траженог софтвера са постојећим инсталираним софтвером на предметној радној станици и уколико оцени да тражени софтвер неће угрозити или ометати рад, инсталираће захтевани софтвер, и то искључиво лиценцирану или бесплатну верзију.

Основна подешавања из става 2. овог члана су:

1) додељивање имена и TCP/IP адресе радној станици и њено придруживање домену;
2) подешавање mail клијента;
3) подешавање web претраживача;
4) инсталација лиценцираног антивирус софтвера, одобреног од стране управе Позоришта;
5) инсталација званичног апликативног софтвера који одређени делови Позоришта користе у свом раду.

У случају да је Кориснику потребно извршити инсталацију одређеног специфичног софтвера на радној станици, електронским путем, подноси образложени захтев директору Позоришта.

Корисник дужан је да сваки проблем у функционисању оперативног система, mail клијента, web претраживача, пословног софтвера (MS Office или Open Office) и апликативног софтвера, пријави директору Позоришта или Овлашћеном лицу директно.

Проблем у функционисању антивирусног софтвера мора се пријавити без одлагања.

Овлашћено лице је дужно да проблеме из става 6. и 7. овог члана отклони у најкраћем могућем року на локацији Корисника, даљинском конекцијом ка радној станици или одношењем радне станице у сервис за поправку.

ЗАВРШНЕ ОДРЕДБЕ

Члан 21.

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

Председник Управног одбора