На основу члана 8. Закона о информационој безбедности („Службени гласник РС“, број 6/16, 94/17 и 77/19), члана 2. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационих система од посебног значаја Владе РС („Службени гласник РС“, број 94/16) и члана 38. Статута ЈП „Стандард“ Јагодина, доносим

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА

Предмет

Члан 1.

Овим Актом ближе се дефинишу мере заштите информационо-комуникационих система Јавног предузећа „Стандард“ Јагодина (у даљем тексту: Предузеће), принципи, начин и процедуре постизања и одржавања високог нивоа безбедности система као и дужности и одговорности корисника информатичких ресурса на Предузећу.

Циљеви

Члан 2.

Циљеви доношења овог правилника су:

1. допринос постизању опште свести о ризицима и опасностима које су везане за коришћење информационих технологија;
2. минимизација безбедоносних инцидената;
3. допринос развоју одговарајућих безбедоносних апликација и обезбеђивање конзистентне контроле свих компонената информационо – комуникационог система (у даљем тексту: ИКТ систем).

Обавезност

Члан 3.

Овај правилник је обавезујући за све унутрашње организационе јединице Предузећа и за све кориснике информатичких ресурса, као и за сва трећа лица која користе информатичке ресурсе Предузећа.

Непоштовање одредби овог правилника од стране корисника информатичких ресурса представља повреду радне обавезе.

За праћење примене овог правилника надлежан је Рачунарски центар Предузећа.

Појмови

Члан 4.

Поједини термини у смислу овог правилника имају следеће значење:

1. интегритет значи очуваност изворног садржаја и комплетности податка;
2. тајност је својство које значи да податак није доступан неовлашћеним лицима;
3. расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

7. кориснички налог јесте корисничко име и лозинка, на основу којих информатички ресурс спроводи аутентификацију (проверу идентитета корисника) и ауторизацију (проверу права приступа, односно овлашћења корисника);

8. администраторски налог јесте јединствен налог који омогућава приступ и администрацију информатичких ресурса само са једним корисничким налогом, као и уношење и измену свих осталих корисничких налога.

Мере заштите

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Предузећа, односно заштита података садржаних у ИКТ систему од неовлашћеног приступа, модификације, коришћења и уништења, на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Информатички ресурси Предузећа

Члан 6.

Информатички ресурси Предузећа су сви ресурси који садрже пословне информације Предузећа 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 обухвата:

1. хардверске и софтверске компоненте информатичких ресурса;
2. податке који се обрађују или чувају на информатичким ресурсима;
3. корисничке налоге за друге податке о корисницима информатичких ресурса Предузећа.

Корисник информатичких ресурса

Члан 8.

Корисник информатичких ресурса јесте лице запослено на одређено или неодређено време у Предузећу, лице ангажовано по основу уговора или друго лице (консултант, студент и сл.) коме је одобрен приступ неком информатичком ресурсу Предузећа.

Корисник информатичких ресурса одговоран је за правилну употребу, тачност и сигурност података приликом коришћења информатичких ресурса Предузећа.

Дужност корисника информатичких ресурса

Члан 9.

Корисник добија информатичке ресурсе на коришћење искључиво у пословне или академске сврхе, а Предузеће задржава право да информатичке ресурсе повуче у одређеном тренутку и у потпуности задржи податке, с тим да ће у том случају Предузеће податке учинити доступним кориснику само уз претходну сагласност директора Предзећа.

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

Корисник радне станице дужан је да пословне податке смешта на локалне непреносиве дискове радне станице или мрежне дискове.

Запослено, односно ангажовано лице у Рачунарском центру Предузећа са администраторским овлашћењима (у даљем тексту администратор) је дужно да повремено израђује резервне копије података са сервера, а док су лица која су задужила поједине радне станице дужна да израђују резервне копије локалних дискова радних станица Предузећа.

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

1. да користи информатичке ресурсе искључиво у пословне, односно академске сврхе;
2. прихвати да су сви подаци који се складиште, преносе или процесуирају у оквиру информатичких ресурса власништво Предузећа и да могу бити предмет надгледања и прегледања;
3. поступа се поверљивим подацима у складу са прописима, а посебно приликом копирања и преноса података;
4. безбедно чува своје лозинке, односно да их не даје другим лицима;
5. мења лозинке сагласно утврђеним правилима;
6. да се пре сваког удаљавања од радне станице одјави са система („log out“ односно „излогује“);
7. обезбеди сигурност података у складу са важећим прописима;
8. приступа информатичким ресурсима само на основу експлицитно додељених корисничких права;
9. не сме да зауставља рад или брише антивирусни програм, мења његове подешене опције, нити да неовлашћено инсталира други антивирусни програм;
10. не сме да на радној станици складишти садржај који не служи у пословне сврхе;
11. израђује заштитне копије (backup) података у складу са прописаним процедурама;
12. користи Internet и Internet e-mail сервис на Предузећа у складу са приписаним процедурама;
13. прихвати да се одређене врсте информатичких интервенција (израда заштитних копија, upgrade firmware, покретање антивирусног програма и сл.) обавља у утврђено време;
14. прихвати да сви приступи информатичким ресурсима и информацијама треба да буду засновани на принципу минималне неопходности;
15. прихвати да технике сигурности (антивирус програми, firewall, системи за детекцију упада, средства за шифрирање, средства за проверу интегритета и др.) спречавају потенцијалну претњу ИКТ систему:
16. не сме да инсталира, модификује, искључује из рада или брише, заштитни, системски или апликативни софтвер;
17. да се уздржи од активности којима се изазива неоправдано оптерећење информатичких ресурса Предузећа, као и повећано ангажовање особља на одржавању тих ресурса;
18. не сме неовлашћено да објављује или преноси личне податке до којих је дошао коришћењем информатичких ресурса Предузећа, као што су лозинке, приватни телефонски бројеви и слично;
19. да се уздржи од неуобичајно и неоправдано великог коришћења информатичких ресурса Предузећа.

Безбедоносни профил корисника информатичких ресурса

Члан 10.

У зависности од описа задатака и послова радног места на које је распоређен, корисник информатичких ресурса, на предлог непосредног руководиоца, стиче одређена права приступа ИКТ систему Предузећа.

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

Креирање лозинке

Члан 11.

Лозинка може да садржи комбиноване карактере од малих и великих слова и цифара.

Лозинка не сме да садржи препознатљиве податке.

Ако корисник информатичких ресурса посумња да је друго лице открило његову лозинку, дужан је да исту одмах измени или, уколико нема приступ, да се писмено обрати администратору који ће лозинку променити.

Употреба корисничких налога

Члан 12.

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

Корисник информатичких ресурса не сме да омогући другом лицу коришћење његовог корисничког налога, осим администратору у случају подешавања радне станице.

Корисник информатичких ресурса је непосредно одговаран 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.

Право коришћења администраторског налога имају администратори за потребе информатичких интервенција.

Поступци у случајевима сигурносних инцидената

Члан 14.

Корисник информатичких ресурса дужан је да, без одлагања, пријави непосредном руководиоцу свако уочавање или сумњу о наступању инцидената којим се угрожава сигурност ИКТ система.

Информације о инциденту руководилац из става 1. овог члана дужан је да одмах проследи администратору, као и Рачунарском центру Предузећа.

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

1. нарушавање поверљивости инфорамција,
2. откривање вируса или грешака у функционисању апликација,
3. вишеструки покушај неауторизованог приступа,
4. системских падова и престанка рада сервиса.

Рачунарски центар Предузећа дужан је да о инциденту који има значајан утицај на нарушавање информационе безбедности обавести директора, у складу са Законом којим се утврђује информациона безбедност.

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...)

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, врши се чишћење 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 коришћења сервиса електронске поште морају се поштовати следећа правила:

1. увек са пажњом приступити свакој поруци у којој се тражи лозинка, никада не уписивати лозинку свог или налога другог лица;

2. никада не отварати додатке (attachments) послате са непознатих адреса;

Поступање са преносивим медијима

Члан 17.

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

Преносив медији из става 1. овог члана, пре 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. сервери и рачунари са посебним апликативним софтвером морају бити смештени у посебним просторијама (припадају одговарајућим Службама Предузећа), које испуњавају стандарде противпожарне заштите, обезбеђене су механичком бравом и у којима је ограничен приступ другим лицима;

2. приступ просторијама из тачке 1. поред лица која су задужена за одржавање ИКТ система и лица која су запослена у тим службама, могу имати и друга лица, уз претходну сагласност директора;

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 инфорамција;

6. медији са поверљивим подацима морају бити заштићени од неауторизованог приступа и прегледа.

Инсталација и одржавање софтвера

Члан 19.

За правилно инсталирање и правилно конфигурисање целокупног софтвера задужени су администратори, који су дужни да поступају у складу са прописаним процедурама и упутствима.

Рачунарски центар Предузећа обезбеђује запосленом, односно другом овлашћеном лицу, коришћење радне станице са преинсталираним и правилно и потпуно конфигурисаним софтвером (оперативни систем, сви управљачи програми (drivers), пословно и развојно окружење, софтвер за вирусну заштиту, разне помоћне апликације), који је типски за све радне станице, који представља минимум потребан за обављање стандардних послова.

Администратор врши процену усклађености траженог софтвера са постојећим инсталираним софтвером на корисничкој радној станици и уколико донесе процену да тражени софтвер неће угрозити рад исте, инсталираће захтевани софтвер.

Основа подешавања из става 2. овог члана су:

1. додељивање имена и TCP/IP адресе радној станици, њено припруживање домену или радној групи;

2. подешавање web претраживача;

3. инсталација одговарајућег антивирусног софтвера;

4. инсталација апликативног софтвера који службе Предузећа користе у свом раду;

Завршна одредба

Члан 20.

Овај правилник ступа на снагу осмог дана од дана објављивања на огласној табли Предузећа.

Надзорни одбор,
Председник