

На основу члана 32. Одлуке о измени оснивачког акта Водопривредног друштва „Сава“ друштво с ограниченом одговорношћу Шабац („Сл. Гласник РС“ бр.78/2018, те чланова 8 Закона о информационој безбедности („Службени гласник РС“, бр. 91/2019, у даљем тексту: Закон), и члана 2 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја (Сл. Гласник РС 94/2016) у даљем тексту:Уредба, вд директора Водопривредног друштва „Сава“ друштво с ограниченом одговорношћу Шабац (у даљем тексту: „ВД „Сава“ ДОО Шабац) дана 21. септембра 2023. године, доноси:

ПРАВИЛНИК О УПРАВЉАЊУ ИНФОРМАЦИЈАМА И БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ВД „САВА“ ДОО ШАБАЦ

Члан 1.

Овим Правилником, у складу са Законом и Уредбом, утврђују се мере заштите, принципи, начини и процедуре у вези са безбедношћу и ресурсима информавионо-комуникационих система Водопривредног деуштва „Сава“ друштва са ограниченом одговорношћу, Шабац (у даљем тексту:Друштва)

Члан 2.

Мере прописане овим Правилником се односе на све Службе Друштва, на све запослене-кориснике информационих ресурса као и на трећа лица која користе информационе ресурсе Друштва.

Мере заштите

Члан 3.

Мерама заштите информационо-комуникационих система(ИКС) се обезбеђује превенција од настанка инцидената, односно, превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављања делатности.

Члан 4.

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

За контролу и надзор над обављањем послова запослених-корисника, у циљу заштите безбедности ИКС, директор Друштва ће у року од 15 дана од дана доношења овог Правилника именовати лице из редова запослених или екстерно ангажовано лице.

Кршење безбедоносних процедура у коришћењу ресурса ИКС-а, запослени-корисник је дужан да пријави лицу из става 2 овог члана, које ће предузети предвиђене мере.

Члан 5.

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 ИКС-а Друштва, као и приступа, измене или коришћење средстава без овлашћења и без евиденције о томе;

У случају инцидента, именовано лице из члана 4 став 2 овог Правилника, обавештава директора Друштва, који, у складу са прописима, обавештава надлежне органе.

Управљање информацијама

Члан 6.

Својинска и ауторска права над информацијама, подацима и софтвером који су креирани коришћењем ИКС ресурса Друштва припадају Друштву. Такође се могу користити програми и софтвери који су изнајмљени и који нису ауторско власништво Друштва.

Сви подаци, независно од форме, који се обрађују, чувају или користе на ИКС ресурсима се класификују према степену поверљивости података.

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

Члан 7.

Када је податак класификован као строго поверљив или поверљив, креиран, све непотребне верзије податаке, настале током креирања, бришу се са радних страница или се уништава папир на коме је штампан.

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

Члан 8.

Слање података класификованих као строго поверљиво или поверљиво, одобрава власник(креатор) података.

Строго поверљиви подаци у електронској форми, шаљу се шифровани, а приликом смештања на преносиви медијум, шифрују се, осим у случају када се достављају лично овлашћеном лицу.

Члан 9.

Уништавање строго поверљивих или поверљивих података, смештених на хард диск врши се коришћењем софтвера за безбедно брисање диска од стране овлашћеног лица.

Уништавањем истих таквих података смештених на преносивом уређају или медијуму врши се форматирањем уређаја или уништењем медијума или уређаја.

Безбедност рада на даљину и употреба мобилних уређаја

Члан 10.

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

Запослени-корисници ИКС-а, могу путем мобилних уређаја, који су у власништву Друштва, да приступе само оним деловима ИКС-а који им омогућавају обављање радних задатака у оквирима њихове надлежности, а уз сагласност директора Друштва.

Члан 11.

Мобилни уређаји морају бити тако подешени да омогућавају сигуран и безбедан приступ, коришћењем мрежа и система, дозвољеним приступом и начином, уз активан одговарајући софтвер за заштиту од вируса и других злонамерних софтвера.

Запосленом-кориснику, забрањено је да самостално инсталирање софтвера и подешавање мобилног уређаја, као и давање уређаја другим неовлашћеним лицима.

Размена електронске поште

Члан 12.

Размена електронске поште у Друштву, дозвољена је искључиво преко система за размену. Систем за размену електронске поште се не сме користити за креирање и дистрибуцију нежељених порука, као ни слање поште, порука са покушајима да се сакрије идентитет пошиљаоца, или представљање као неко други.

Члан 13.

Забрањено је употреба службене адресе електронске поште за размену порука, чији је садржај увредљив, клеветнички, или застрашујући, као и погрдан према било коме, које су дискриминативне, којима се откривају пословне тајне Друштва, или пословних партнера, које служе у политичке или сличне пропагандне сврхе, као и поруке које својим садржајем ометају запослене у раду, или изазивају друге врсте сметњи.

Нежељена пошта се смешта у карантин.

Није дозвољено слање електронских порука без наслова или већих димезија(дужине) од прописане.

Оспособљавање лица које управља ИКС-ом

Члан 14.

Коришћењем ИКС-ом управља лице које је решењем директора по члану 4 овог Правилника одређено.

Сваки новозапослени се упознаје са функционисањем система у оквиру његових радних задатака, одговорношћу које то носи.

Свака врста злоупотребе запослених при коришћењу ИКС-а, ван додељених овлашћења и оквира посла, подлеже дисциплинској одговорности.

У случају промене послова у оквиру Друштва, врши се усклађивање приступа

ИКС-у у складу са новим пословима.

Приликом престанка радног односа, налози и привилегије приступа ИКС-у се укидају, а бивши запослени не сме да открива податке које су од значаја за информациону безбедност.

Информациона добра и њихова заштита

Члан 15.

Информациона добра Друштва сви ресурси који садрже пословне информације, укључујући све електронске записе, рачунарску опрему, мобилне уређаје, базе података, пословне апликације, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње правилнике и сл.

Предмет заштите су хардверске и софтверске компоненте ИКС-а, подаци који се обрађују и чувају на компонентама ИКС-а, кориснички налози и други подаци о корисницима информатичких ресурса.

У циљу заштите ИКС-а, одговорно лице организује начин и приступ и ресурсима и систему, поготово подацима који представљају службену тајну, а у складу са Законом који то регулише.

Ограничење приступа подацима, систему и средствима

Члан 16.

Приступ ресурсима ИКС-а одређена је врстом налога, односно додељеном улогом коју запослени-корисник има, зависно од посла који у Друштву обавља.

Запослени-корисник може да користи само свој кориснички налог, уз поштовање свих безбедоносни норми, и не може дозвољавати приступ и коришћење другим лицима, сем у случајевима Правилником дозвољеним, и свака врста злоупотребе подлеже кривичној и дисциплинској одговорности.

Члан 17.

Кориснички налог се састоји од корисничког имена и лозинке, који служе за идентификацију и приступ систему.

Лозинка мора да садржи:

- Број карактера који је већи од осам
- Најмање једно велико слово
- Најмање један број

Лозинка не сме да садржи име, презиме, датум рођења, број телефона и друге препознатљиве податке. У случају да се посумња да је лозинка откривена, дужан је запослени исту одмах променити. Лозинка се мења на сваких 6 месеци.

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

Запослени-корисник користи квалификоване електронске сертификате за електронско потписивање докумената као и аутентификацију и ауторизацију приступа појединим апликацијама, на инсталираним софтверима и хардверима за коришћење сертификата и потписа, и запослени посебно треба да чувају приступ оваквог начина коришћења система.

Заштита података и опреме

Члан 18.

Опрема мора бити заштићена од сваке врсте оштећења, нестанка ел енергије, морају постојати процедуре о изношењу и поправци опреме, заштити података приликом сервисирања и поправки.

По потреби, када прилике налажу, прави се копија-архива постојећих података.

Заштита од злонамерног софтвера на мрежи се спроводи у циљу заштите од вируса и других врста злонамерног кода који у рачунарску мрежу може доспети интернет конекцијом, имејлом, зараженим преносним медијима (УСБ меморија, ЦД-ом) и слично.

За заштиту од вируса на сваком рачунару се инсталира антивирус програм.

Забрањено је са пословних рачунара, посећивати сумњиве web странице, гледати филмове, преузимање података велике тежине, као и сваку другу врсту непримереног коришћења рачунарске опреме и приступање садржајима који нису везани за посао.

Члан 19.

Базе података обавезно се архивирају и на преносиве медије (ЦД РОМ, ДВД, УСБ, екстерни хард диск), најмање једном месечно, за потребу обнове базе података.

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

У ИКС-у се може користити само лиценцирани софтвер.

При свакој инсталацији нове верзије софтвера или подешавања, неопходно је направити копије постојећег, како би се обезбедила могућност повратка на претходно стање у случају неочекиваних ситуација или компликација.

Ревизија ИКС-а се мора вршити тако да што мање омета пословне процесе, по потреби и после краја радног времена или викендом.

Члан 20.

Инсталација, замена или одржавање ресурса ИКС-а од стране трећих лица, која нису запослена у овом Друштву, или ангажованих правних лица, њихова одговорност и обавеза чувања тајни које сазнају у раду, биће дефинисана уговором са тим лицима.

Трећа лица, пружаоци услуга, могу приступити само оним подацима који се налазе у базама података које су део софтвера који су они израдили.

Члан 21.

У случају било каквог инцидента који угрожава рад и безбедност ИКС-а, запослени-корисник је дужан да обавести одговорно лице које је именовано одлуком директора, по овом Правилнику, а по потреби и директора Друштва.

Уколико се ради о инцидентима који су дефинисани Уредбом, обавештавају се и надлежни органи, дефинисани овом Уредбом.

У случају ванредних околности, могуће је да дође до измештања Друштва на резервну локацију, у том случају и ИКС се са највећом пажњом измешта, био цео, или делови, на резервну локацију.

Прелазне и завршне одредбе

Члан 22.

Овај Правилник се објављује на огласној табли Друштва, и ступа на снагу у року од 8 дана од објављивања на огласној табли.

Вд Директора

Ненад Мишковић