Привредно друштво за рекултивацију и озелењавање земљишта "РИО" Д.О.О. КОСТОЛАЦ
Николе Тесле б.б. 12208 Костолац | Веб: www.riokostolac.rs | Е-маил:
office@riokostolac.rs Телефони: +381 (12) 241-568 и (12) 242-105 | Факс: +381 (12) 241-568

На основу члана 16. Одлуке о измени оснивачког акта Привредног друштва за рекултивацију и озелењавање земљишта "РИО" доо Костолац бр. 67 од 26.10.2016. године, Директор "РИО" доо Костолац доноси:

ПРАВИЛНИК
о начину рада, вођења и коришћења информационог система и његовој садржини

Уводне одредбе

Члан 1.

Овим правилником прописује начин рада, вођења и коришћења информационог система у Привредном друштву за рекултивацију и озелењавање земљишта "РИО" доо Костолац.

Члан 2.

Мере прописане овим правилником се односе на све запослене - кориснике информатичких ресурса.

Члан 3.

Поједини термини у смислу овог правилника имају следеће значење:

1) информациони систем (ИТ 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 воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИТ системом;

2) информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИТ 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;

3) тајност је својство које значи да податак није доступан неовлашћеним лицима;

4) интегритет значи очуваност изворног садржаја и комплетности податка;

5) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) 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;

7) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

8) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИТ система;

9) 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;

10) инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

11) мере заштите ИТ система су техничке и организационе мере за управљање безбедносним ризицима ИТ система;

12) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

13) ИТ систем за рад са тајним подацима је ИТ систем који је у складу са законом одређен за рад са тајним подацима;

14) безбедносна зона је простор или просторија у којој се, у складу са прописима чувају подаци;

15) информациона добра обухватају податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште правилнике, процедуре и слично;

16) Download је трансфер података са централног рачунара или web презентације на локални рачунар;

17) UPS (Uninterruptible power supply) је уређај за непрекидно напајање електричиом енергијом;

18) Freeware је бесплатан софтвер;

19) Opensource софтвер отвореног кода;

20) 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;

21) USB или флеш меморија је спољашњи медијум за складиштење података;

22) CD-ROM (Compact disk - read only memory) се користи као медијум за снимање података;

23) DVD је оптички диск високог капацитета који се користи као медијум за складиштење података.

Члан 4.

Послове одржавања ИТ система врши лице запослено на радном месту сарадник за административну и информатичку подршку, лице ангажовано по уговору или запослени по налогу директора.

Мере заштите

Члан 5.

Мерама заштите ИТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају обављање делатности.

Члан 6.

Сваки запослени-корисник ресурса ИТ система је одговоран за безбедност ресурса ИТ система које користи ради обављања послова и делокруга свога рада.

Члан 7.

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 управљање ризицима у области информационе безбедности, као и послови предвиђени процедурама у области информационе безбедиости,
- послови онемогућавања, односно спречавања неовлашћене или ненамерне измене, оштећења или злоупотребе средстава, односно информационих добара ИТ система Привредног друштва "РИО" доо, као и приступ, измене или коришћење средстава без овлашћења и без евиденције о томе,
- бекап података неопгодних за обављање делатности,
- спречавање изношења тајних података изван ИТ система Привредног друштва "РИО" доо.

Члан 8.

У случају промене описа послова корисника-запосленог, лице задужено за послове одржавања ИТ система ће извршити промену привилегија које је корисник - запослени имао у складу са описом радних задатака, а на основу налога директора Привредног друштва.

Корисник ИТ ресурса, након престанка радног ангажовања у Привредном друштву "РИО" доо Костолац , не сме да открива податке који су од значаја за информациону безбедност ИТ система.

Заштита података и средства за обраду података од злонамерног софтвера

Члан 9.

Заштита од злонамернаг 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 (USB меморија, CD итд.}, инсталацијом нелиценцираног софтвера и сл.

За успешну заштиту од вируса на сваком рачунару је инсталиран антивирусни програм. Свакодневно се аутоматски врши допуна аитивирусних дефиниција, а најмање једном месечно.

Забрањено је заустављање и искључивање антивирусног софтвера таком скенирања преносивих 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 анти вирусним софтвером.

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

У циљу заштите, одиосно упада у ИТ систем Привредног друштва "РИО" доо са интернета, запослени или лице ангажовано на пословима одржавања рачунара, је дужан да одржава систем за спречавање упада.

Корисници ИТ система који користе интернет морају да се придржавају мера заштите од вируса и упада са интернета у ИТ систем, а сваки рачунар чији се залослени-корисник прикључује на Интернет мора бити одговарајуће подешен и заштићен, при чему подешавање врши запослени или лице ангажовано на пословима одржавања рачунара.

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

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави лицу запосленом или ангажованом на радном месту одржавања рачунара.

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 начии 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);
- недозвоњено коришћење друштвених мрежа и других интернет садржаја које је ограничено;
- преузимање (download) података велике "тежине" које проузрокује "загушење" на мрежи;
- преузимање (download) материјала заштићених ауторским правима;
- коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и сл.);
- недозвољени приступ, промена, брисање или прерада садржаја преко интернета.

Заштита од губитка података
Обезбеђивање интегритета софтвера и оперативних система

Члан 10.

Инсталацију и подешавање софтвера може да врши запослени на радном месту одржавања рачунара, запослени по овлашћењу директора 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 података у комуникационим мрежама укључујући уређаје и водове

Члан 11.

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, rnuter, firewalZ), која се налази у просторијама Привредног друштва "РИО" доо, се мора налазити у закључаном rack орману.

Безбедност података који се преносе унутар оператера ИТ система, као и између оператера ИТ система и лица ван оператера ИТ система.

Члан 12.

Размена података са Трезором, Пореском управом, Централним регистром социјалног и здраветвеноаг осигурања, Управом за јавне набавке, Агенцијом за борбу против корупције и сличним институцијама са којом се врши размена података у складу са Уговором (протоколом).

Запослени који имају администраторске или корисничке налоге.

Члан 13.

Запослени у Привредном друштву "РИО" доо који имају кориснички или административни налог су:

1. За рад на Порталу Централног регистра социјалног осигурања референт за правне, кадровске и административне послове а у његовом одсуству запослени по налогу одговорног лица.

2. За рад на порталу Пореске управе и ЛПА управе, Руководилац службе за економске и финансијске послове, референт рачуноводствених послова и ликвидатор - обрачунски радник.

3. За рад на систему СЕФ одговорно лице, секретар руководилац службе за економске и финансијске послове, референт рачуноводствених послова и ликвидатор - обрачунски радник.

4. За рад на Порталу јавних набавки по налогу одговорног лица,

5. За рад на веб сајту Привредног друштва "РИО" доо задужен је сарадник за административну и информатичку подршку,

6. За рад на пословном софтверу Archilleus привилегије су дефинисане одобрењем одговорног лица.

Прелазне и завршне одредбе

Члан 14.

Привредно друштво за рекултивацију и озелењавање земљишта "РИО" Д.О.О. КОСТОЛАЦ
Николе Тесле б.б. 12208 Костолац | Веб: www.riokostolac.rs | Е-маил:
office@riokostolac.rs Телефони: +381 (12) 241-568 и (12) 242-105 | Факс: +381 (12) 241-568

Правилник као и Измене и дапуне овог Правилника доноси одговорно лице Привредног друштва "РИО" доо Костолац.

Члан 15.

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

ДИРЕКТОР
ПД "РИО" доо Костолац
Игор Газдић

Правилник је објављен на огласној табли Привредног друштва "РИО" доо 2023. године,

а ступа је на снагу _____. године.