ЈАВНО КОМУНАЛНО ПРЕДУЗЕЋЕ
3.ОКТОБАР БОР
Адреса: 7 јули бр.60, Бор 19210, Србија
Телефон: +381 30 432224; +381 30 441698
Е адреса: jkp.3oktobar.bor@gmail.com
Датум: 02.07.2024 .год
Број: 1200

На основу чл.8 Закона о информационој безбедности ("Сл.гласник РС" бр. 6/16, 94/17 и 77/19) и чл.29. Статута Јавног комуналног предузећа „3.октобар" Бор и чл.192.став 1.тачка 1. Закона о раду („Сл.гласник РС" бр. 24/05 61/05, 54/09, 32/2013, 75/2014, 113/2017 и 95/2018 -АТ), доносим

ПРАВИЛНИК О УПРАВЉАЊУ ИНФОРМАЦИЈАМА (ПОДАЦИМА) И БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА У ЈАВНОМ КОМУНАЛНОМ ПРЕДУЗЕЋУ „3.ОКТОБАР" БОР

Предмет регулисања

Члан 1.

Овим правилником ближе се уређује управљање информацијама (подацима) у Јавном комуналном предузећу "3.октобар" Бор, приступ, коришћење података и опреме, мере заштите и контрола, обнова, уништавање података и опреме, и чување података као поверљивих .

Члан 2.

Мере прописане овим правилником односе се на све радне јединице Јавног комуналног предузећа "3.октобар" Бор, на све запослене кориснике информатичких ресурса као и на трећа лица која користе информатичке ресурсе Јавног комуналног предузећа "3.октобар" Бор.

Приступ и коришћење информационо-комуникационог система предузећа

Члан 3.

Право приступа подацима и коришћења опреме информационо-комуникационог система предузећа имају само запослени који имају корисничке и администраторске налоге и приступне шифре.

Отварање корисничких налога и приступних шифара врши се само по одобрењу директора.

Администраторска права и овлашћења за приступ даје директор, или руководилац радне јединице по предходном одобрењу од стране директора.

Запослени приступају информацијама и користе опрему и информационо-комуникациони систем предузећа само у обављању редовних пословних активности.

Забрањен је приступ информацијама, опреми и коришћење информационо-комуникационог система ван раног процеса у циљу задовољавања личних потреба и интереса.

Мере заштите и контроле

Члан 4.

Мере заштите информационо-комуникационог система подразумевају мере којима се врши превенција настанка инцидената који угрожавају обављање делатности предузећа.

У циљу заштите информационо-комуникационог система у предузећу се спроводе следеће мере:

- запослени су дужни да чувају у тајности лозинке и шифре за приступ рачунарима, као и шифре за идентификацију у информационо-комуникациони систем Јавног комуналног предузећа "3.октобар" Бор
- запослени су дужни да лозинке и шифре редовно ажурирају једанпут у шест месеци
- уколико запослени посумња да је друго лице открило његову лозинку дужан је да исту одмах измени
- запослени су дужни да чувају податке корисника услуга и пословних партнера предузећа
- копије података чувају ее на екстерним хард дисковима изван просторија предузећа по предходном одобрењу од стране директора и klaud serverima (google drive) (као мере заштите за случај пожара, поплаве и других елементарних непогода)
- сваки запослени - корисник информационо-комуникационог система одговоран је за безбедност ресурса информационо-комуникационог система које користи у обављању послова из своје надлежности
- за контролу у циљу заштите и безбедности информационо-комуникационог система одговорно је запослено лице у чијем је опису послова одржавање информационо - комуникационог система предузећа
- сваки запослени је дужан да одмах пријави кршење безбедоносних процедура у информационо-комуникационом систему лицу одговорном за контролу и директору ради предузимања одговарајућих мера и обавештавања надлежних органа
- референт за радне односе обавештава лице задужено за контролу уколико дође до престанка радног односа лица које је у свом раду користило информатичке ресурсе ради укидања корисничког налога и приступних привилегија тог запосленог.

Обнова опреме

Члан 5.

Обнова опреме врши се на захтев корисника за набавком опреме уз учешће лица одговорног за контролу и уз предходно одобрење од стране директора.

У изради техничке спецификације за набавку опреме поред запосленог обавезно учествује и лице одговорно за контролу у чијем је опису послова одржавање информационо - комуникационог система предузећа.

Инсталирање нове опреме врши лице задужено за контролу.

Класификација података као поверљивих и уништавање података

Члан 6.

Подаци који су настали у раду, који се размењују, чувају или обрађују коришћењем информационо-комуникационог система, без обзира у којој форми се налазе могу се класификовати према степену поверљивости података. Одлуку о поверљивости одређених података доноси директор.

Уколико запослени користи поверљиве податке дужан је да их штити у свим фазама коришћења и одговоран је за поступање са њима.

Уколико је податак класификован као строго поверљив или поверљив, све непотребне верзије података бришу се са радне станице и уништава се папир на коме је податак или информација штампана (сецкањем, цепањем) у присуству комисије именоване од стране директора.

Подаци који су у електронској форми а који су класификовани као строго поверљиви или поверљиви чувају се на серверима у директоријумима са ограниченим правом приступа.

Уништавање података који су класификовани као строго поверљиви или поверљиви а који су смештени на хард диску врши се помоћу софтвера за безбедно брисање диска од стране лица задуженог за контролу.

Члан 7.

Овај Правилник ступа на снагу даном доношења и објављује се на огласној табли и интернет страници предузећа.

Објављен Правилник на огласној табли дана 02.07.2024. године

В.Д. Директора

Ненад Крачуновић, дипл.инж.шум.