ПОЛИТИКА БЕЗБЕДНОСТИ ИНФОРМАЦИЈА

ЈКП "БЕОГРАДСКИ ВОДОВОД И КАНАЛИЗАЦИЈА"

ISMS ISO/IEC 27001:2022

Систем управљања безбедношћу информација, у складу са захтевима ISO/IEC 27001, успостављен је у циљу обезбеђивања неометаног пословања, уз адекватну заштиту поверљивих информација, без обзира на њихов облик и начин чувања. Наведено се постиже кроз заштиту информација и имовине која је у вези са информацијама предузећа, од уочених унутрашњих или спољашњих претњи, кроз адекватну примену, праћење, преиспитивање, одржавање и побољшање ISMS-а као дела успостављеног система менаџмента.

Стално побољшање безбедности информација, кроз развој информационог система, поступака и свести запослених, доводи до раста задовољства корисника пруженим услугама и квалитетом саме услуге, као и поверења да су информације корисника и других заинтересованих страна заштићене.

Кроз ову политику, која представља као оквир за успостављање циљева безбедности информација, руководство исказује своју опредељеност за следеће:

- ***Стално побољшање пракси безбедности информација, уз примену савремених информационих решења,***
- ***Одржавање поверљивости, расположивости и интегритета информација, у складу са дефинисаном шемом класификације информација,***
- ***Омогућавање приступа искључиво информацијама које су неопходне за пружање услуга и реализацију пословних активности,***
- ***Спречавање неовлашћеног приступа информацијама, кроз адекватну логичку заштиту података, софтвера, информационе инфраструктуре, али и физичких локација предузећа,***
- ***Очување интегритета информација кроз контролу приступа по принципу „треба да зна“ и привилегије корисника који им приступају,***
- ***Контролисан приступ испоручиоца поверљивим информацијама предузећа, кроз адекватно информисање и уговоре о поверљивости података,***
- ***Стално стручно усавршавање и оспособљавање запослених кроз обуке и едукацију,***
- ***Праћење и анализу инцидената безбедности информација, као и учење из истих,***
- ***Примену планова континуитета пословања, у случајева постојања поремећаја,***
- ***Усаглашеност са свим примењивим захтевима закона, прописа, правилника и уговора, посебно узимајући у обзир да смо предузеће од јавног значаја .***

Руководство ЈКП "Београдски водовод и канализација" је посвећено сталном унапређењу система управљања безбедношћу информација и обезбедиће да ова политика буде саопштена свим запосленима и заинтересованим странама, примењена и редовно преиспитана. Сви запослени су дужни да се придржавају одредби ове политике и упознати са својим одговорностима у случају нарушавања безбедности информација.

У остваривању наведених циљева очекујем максималан допринос свих запослених

Директор Сектора за интегрисани систем квалитета

Марија Петровић

ВД ДИРЕКТОРА

Радомир Вујадин

Београд, 12.08.2024.год.

ISMS ISO 27001:2022

ПОЛИТИКА КОНТИНУИТЕТА ПОСЛОВАЊА
ЈКП "БЕОГРАДСКИ ВОДОВОД И КАНАЛИЗАЦИЈА"

- ЈКП "Београдски водовод и канализација"је донео ову Политику у циљу обезбеђивања континуитета менаџмента безбедношћу информација у неповољним ситуацијама (попут криза, ратова, катастрофа, ванредних ситуација и непогода).

- Основни план континуитета се реализује кроз постојање две физички одвојене локације – примарне и секундарне.

- Главне потенцијалне ванредне ситуације које се могу јавити у ЈКП "Београдски водовод и канализација" су пад/неисправност сервера, нестанак струје, природне непогоде и политичка нестабилност у држави и региону.

- ЈКП "Београдски водовод и канализација"је опремљен UPS-евима и агрегатима, редовно врши „backup“ својих података, запослени су високо стручни и припремљени за реаговање у ванредним ситуацијама, а све у циљу обезбеђивања континуитета пословања.

- ЈКП "Београдски водовод и канализација" периодично спроводи симулације поступања у неповољним ситуацијама, и том приликом се од свих запослених очекује максимална посвећеност и труд, како би цела организација била што боље припремљена за реаговање у ванредним ситуацијама.

У остваривању наведених циљева очекујем максималан допринос свих запослених

Директор Сектора за интегрисани систем квалитета

Марија Петровић

В Д ДИРЕКТОРА

Радомир Вујадин

Београд, 12.08.2024.год.

ISMS ISO 27001:2022

ПОЛИТИКА КОРИШЋЕЊА САВРЕМЕНИХ ТЕХНОЛОГИЈА ЈКП "БЕОГРАДСКИ ВОДОВОД И КАНАЛИЗАЦИЈА"

Запослени у ЈКП "Београдски водовод и канализација" су приликом коришћења опреме и технологија за обраду и/или размену информација у обавези да:

1892

- ***Никада опрему не дају на коришћење/употребу лицима која ЈКП "Београдски водовод и канализацијa" није препознала као овлашћена,***
- ***Никада опрему не остављају без надзора у присуству лица која ЈКП "Београдски водовод и канализацијa" није препознала као овлашћена,***
- ***Посвете посебну пажњу приликом коришћења и приступања VPN-у,***
- ***Не приступају друштвеним мрежама и другим програмима на интернету коју би могли на било који начин да доведу у опасност поверљивост, интегритет и/или доступност информација ЈКП "Београдски водовод и канализација",***
- ***На својим приватним профилима на друштвеним мрежама никад не објављује коментаре, слике и слично у вези са пословањем ЈКП "Београдски водовод и канализација",***
- ***Пословни мејл користе само и искључиво у пословне сврхе,***
- ***Никада не користе приватне мејлове за размену података и информација које се на било који начин односе на пословање ЈКП "Београдски водовод и канализација".***

У остваривању наведених циљева очекујем максималан допринос свих запослених

Директор Сектора за интегрисани систем квалитета

Марија Петровић

В Д ДИРЕКТОРА

Радомир Вујадин

Београд, 12.08.2024.год.

ISMS ISO 27001: 2022

ПОЛИТИКА ЧИСТОГ СТОЛА И ЕКРАНА

ЈКП "БЕОГРАДСКИ ВОДОВОД И КАНАЛИЗАЦИЈА"

У циљу подизања нивоа безбедности информација, као и целокупне свести о овом појму код запослених у ЈКП „Београдски водовод и канализација“ донета је ова Политика.

Од свих запослених у ЈКП „Београдски водовод и канализација“се очекује да:

- ***Приликом свакодневних активности на столу/екрану држе и користе само она документа која су им у том тренутку потребна за рад,***
- ***Осим докумената у папирном облику ово правило се односи и на све облике чувања електронских података, попут CD, DVD и USB меморија,***
- ***Након завршетка активности, сва документа и сви преносни електронски медији за складиштење се одлажу на за то предвиђена места,***
- ***Приликом састанака и других сличних активности, сва поверљива документа држе ван видокруга и домашаја неовлашћених лица,***
- ***Уколико се ради о презентацијама неопходно је онемогућити све “pop up“-ове и са радне површине екрана склонити сва документа у фолдере који нису видљиви на радној површини екрана,***
- ***Приликом привременог напуштања радног места, сва документа одложе и склоне на за то предвиђена места. Такође, неопходно је одјавити се са рачунара,***
- ***Након истека радног времена, одложе и склоне сва документа на за то предвиђена места и угасе рачунаре (на којима постоје шифре),***
- ***Поштују ову политику као и сва остала проглашена документа система менаџмента безбедношћу информација,***
- ***Сваки документ који се пошаље на штампач треба одмах узети са штампача да би се спречио неовлашћен приступ и потенцијална злоупотреба информација.***

У остваривању наведених циљева очекујем максималан допринос свих запослених

Директор Сектора за интегрисани систем квалитета

Марија Петровић

ВД ДИРЕКТОРА

Радомир Вујадин

Београд, 12.08.2024.год.

ПОЛИТИКА КОНТРОЛЕ ПРИСТУПА

Политика контроле приступа је документ, који уз Правилник о безбедности информационо-комуникационих система ЈКП „Београдски водовод и канализација“, утврђује начин управљања приступом системима и информацијама.

Опште

Приликом дизајнирања контроле приступа за системе и активности Предузећа, користе се општи принципи и то:

• „Нужно је знати“ („Need to know“) – приступ информацијама које су неопходне за обављање задатака и

• „Нужно је користити“ (“need to use”) – одобрен је приступ опреми за обраду информација (ИТ опрема, апликације, собе) да би се извршио задатак/посао.

Поштовање ових основних принципа помаже да се системи одрже безбедним смањењем рањивости, а самим тим и смањењем броја и озбиљности безбедносних инцидената који се могу десити.

Управљање корисничким приступом

Ова политика се примењује за сваку апликацију и информациони систем како би се обезбедио ауторизовани приступ корисника и спречио неовлашћени приступ. Примењује се на све фазе животног циклуса корисничког приступа, од почетне регистрације нових корисника до коначне одјаве корисника којима приступ више није потребан.

Права приступа корисника се ревидирају у редовним интервалима како би се осигурало да су одговарајућа права и даље додељена.

Администраторски налог имају само лица која су задужена за одржавање ИКТ ресурса у Предузећу.

Регистрација и одјава корисника

Захтев за приступ мрежи и рачунарским системима подноси се у писаној форми Сектору за ИКТ. Сви захтеви се обрађују према дефинисаној процедури која обезбеђује да се спроведу одговарајуће безбедносне провере и добије исправна ауторизација пре креирања корисничког налога. Принцип поделе дужности је примењен јер захтев за креирање корисничког налога и доделу приступа и спровођење таквог захтева обављају различите функције (особе).

Сваки кориснички налог има јединствено корисничко име које се не дели ни са једним другим корисником и повезано је са одређеном особом, а не са функцијом односно радним местом. Групне налоге потребно је избегавати где год је то могуће јер не обезбеђују јасну поделу одговорности.

ПОЛИТИКА КОНТРОЛЕ ПРИСТУПА

Када запослени напусти Предузеће под нормалним околностима, његов приступ рачунарским системима и подацима се укида на крају радног дана последњег радног дана запосленог. Захтев за укидање се доставља Сектору за ИКТ од стране Кадровске службе.

У изузетним околностима у којима се сматра да постоји ризик да запослени може предузети радње које могу да нашкоде Предузећу пре или након раскида радног односа, захтев за укидање приступа се може одобрити и предузети мере пре обавештења о раскиду радног односа. Ова мера предострожности ће се посебно применити у случају када појединац има привилегована права приступа, нпр. администраторски налог.

Кориснички налози морају бити у почетку само укинути или онемогућени, а не обрисани. Називи корисничких налога се не смеју поново користити јер то може изазвати забуну у случају евентуалне истраге о било којој сумњивој ситуацији.

Омогућавање корисничког приступа

Сваком кориснику морају бити додељена права приступа рачунарским системима и подацима који су сразмерни задацима и активностима повезаним са њиховим радним местом односно функцијом и принципима наведеним у овој политици.

Укидање или прилагођавање права приступа

Тамо где је потребно прилагођавање права приступа, нпр. због промене радног места или функције појединца мора се осигурати да се права приступа која више нису релевантна укину са корисничког налога. Исти принцип важи ако корисник преузима нову улогу поред своје постојеће.

Ни под којим околностима администраторима није дозвољено да мењају сопствене корисничке налоге или дозволе.

Управљање правима привилегованог приступа

Привилегована права приступа морају бити идентификована за сваки систем или мрежу и строго контролисана. Ови налози су специфични за појединца; групни администраторски налози се не смеју користити јер не пружају јасну поделу корисника.

Провера права приступа

На редовној основи (најмање једном годишње) врши се провера права приступа. Ово обезбеђује да се идентификују особе који не би требало да имају приступ (нпр. они који су напустили Предузеће), кориснички налози са више приступа него што то захтева њихово радно место или функција, кориснички налози са погрешним додељивањем приступа, кориснички налози који не пружају адекватну идентификацију (нпр. групни налози) или било које друге ситуације која нису у складу са овом политиком. Резултати провере права приступа се документују у одговарајућем извештају.

ПОЛИТИКА КОНТРОЛЕ ПРИСТУПА

Ако се утврди било каква неусаглашеност као резултат спроведене провере, она се мора отклонити и применити процедура за управљање корективним мерама.

Политика аутентификације

Уколико се, на основу анализе ризика, процени да је потребно могу се користити додатне методе аутентификације. Коришћење додатних аутентификација узима у обзир вредност штићене имовине, процењени степен опасности, трошак додатних аутентификација, употребу и практичност предложених метода, као и све друге контроле које се већ користе.

Без обзира да ли се користи једнострука или вишефакторска аутентификација, квалитет корисничких лозинки мора да се спроводи у свим мрежама и системима користећи принципе политике лозинки.

Контрола приступа систему и апликацијама

Ефективна контрола приступа и примена одговарајућих мера обухвата свеобухватни безбедносни модел који укључује: креирање индивидуалних корисничких налога, дефинисање улога или група којима се могу доделити кориснички налози, додељивање дозвола различитих типова (нпр. читање, писање, брисање, извршавање), обезбеђивање различитих приказа опција менија и података у складу са корисничким налогом и нивоима приступа, администрација корисничког налога, контроле за пријаву корисника, временско ограничење неактивности корисника, управљање лозинкама, као пријављивање/ одјављивање, неуспешне покушаје пријављивања.

Приступ мрежама и мрежним услугама

Предузеће примењује систем firewall како би заштитило периметре мреже од неовлашћеног приступа. Дизајн firewall обезбеђује сегрегацију мрежа информационих услуга корисника и информационих система.

Приступ крајњих уређаја локалној мрежи могућ је само на два начина: из канцеларије Предузећа или са удаљене локације, користећи VPN везу.

У остваривању наведених циљева очекујем максималан допринос свих запослених

Директор Сектора за интегрисани систем квалитета

Марија Петровић

ВД ДИРЕКТОРА

Радомир Вујадин

Београд, 12.08.2024.год.