ПРОЦЕДУРА

УПРАВЉАЊЕ ПРИСТУПОМ

Израдио: Петар Јовановић

Контролисао: Милован Жагрић

Процедура је обавезна за примену. Дужност сваког запосленог на кога се процедура односи је да се са истом упозна и поступа на прописан начин. Обавезна је примена свих упутстава и записа који су дефинисани овом процедуром.

Датум: 20.09.2018.

Директор: Дејан Јонић

Одговоран за примену: **Помоћник директора/Представник руководства за систем менаџмента и Заменик представника руководства**

Одговоран за измене у процедури: **Помоћник директора/Представник руководства за систем менаџмента и Заменик представника руководства**

1. ПРЕДМЕТ

Предмет ове процедуре је дефинисање поступака и документације у процесу управљање приступом.

2. ПОДРУЧЈЕ ПРИМЕНЕ

Ову процедуру примењују сви запослени у Сектору за информатичку подршку.

3. ДЕФИНИЦИЈЕ И СКРАЋЕНИЦЕ

- „ISMS" – „Information Security Management System" - Систем управљања безбедношћу информација;
- ИТ – информационе технологије;
- УЗЗПРО – Управа за заједничке послове републичких органа.
- **Приступ** – Термин приступ који се користи у оквиру ове процедуре обухвата како физички приступ различитим локацијама, тако и приступ апликацијама.
- **Право приступа** – могућност да се приступи одговарајућим ресурсима уз извесна ограничења, одговорности и овлашћења.
- **МУП** – Министарство унутрашњих послова.

4. ВЕЗА СА ДРУГИМ ДОКУМЕНТИМА

Интерна:

- **ПОСЛОВНИК КВАЛИТЕТА**;
- **ПОСЛОВНИК БЕЗБЕДНОСТИ ИНФОРМАЦИЈА**;
- Процедура **ВОЂЕЊЕ ПОСЛОВА ФИЗИЧКО-ТЕХНИЧКОГ ОБЕЗБЕЂЕЊА**;
- Процедура **ВОЂЕЊЕ ПОСЛОВА ЗАШТИТЕ ОД ПОЖАРА**;
- Документа QMS-а и ISMS-а;

Екстерна:

- ISO 9000:2015, Системи управљања квалитетом - основе и речник, 2015. година;
- ISO 9001:2015, Системи управљања квалитетом - захтеви, 2015. година;
- ISO 9004:2009, Системи управљања квалитетом - упутства за побољшање перформанси, 2009. година;
- ISO/IEC 27001:2013, Информационе технологије – Технике безбедности – Системи менаџмента безбедношћу информација – Захтеви.

5. ОПИС ПРОЦЕДУРЕ

5.1 Додељивање и укидање права приступа

Захтев за доделу права приступа могу поднети сви запослени. Одлуку о додели права приступа доноси Директор УЗЗПРО. У захтеву који се формира као електронска пошта морају се навести подаци о лицу које подноси захтев, као и област за коју се приступ захтева са објективним разлогом потребе за дозволом приступа. Такође, на сваких шест месеци се од стране Начелника одељења за системско-техничку подршку, врши преиспитивање постојећих (издатих) права приступа, који су дати у оквиру записа ***Конторла приступа***, и по потреби врши њихово проширивање или смањење. Такође, на сваких шест месеци, власници имовине којој се додељује право приступа врше преиспитивање права приступа истој и врше, по потреби, проширење или смањење тих приступа. Сви имаоци права приступа (како они „регуларни", тако и „привилеговани") могу приступити једино ресурсима за која имају овлашћење да користе и сваки други покушај ће бити сматран нарушавањем интегритета система безбедности информација и у том случају је потребно покренути одговарајуће мере.

Сви запослени, као и испоручиоци, приликом запослења, као и на сваких шест месеци пролазе безбедносну проверу од стране МУП и осталих одговарајућих служби како би им се омогућио уопште физички приступ згради у Немањиној 22-26.

Свим запосленима, као и испоручиоцима, по престанку трајања уговора престају да постоје и права приступа. Такође, исти су дужни да раздуже/укину све везе са евентуалним могућностима остварења права приступа (корисничка имена, лозинке, картице итд.). Такође, приликом измена у оквиру уговора са запосленима и испоручиоцима, мора се преиспитати статус овлашћења у погледу приступа.

5.2 Управљање приступом

УЗЗПРО као вид безбедности информација, води рачуна о физичкој безбедности и раздвојености различитих делова организације. Сваки посетилац УЗЗПРО је дужан да приликом уласка у зграду организације прође безбедносне процедуре прописане од стране МУП-а. Запослени из МУП-а на пријавници води евиденцију свих посетилаца (име и презиме, број личне карте, код кога се посетилац запутио, врема када је дошао, као и време када је напустио организацију). Улаз у зграду у којој се налази УЗЗПРО 24 сата дневно чува обезбеђење делегирано од стране МУП-а.

Како би се заштитиле области у којима се налазе осетљиве или критичне информације и опрема, дефинисани су и користе се адекватне безбедоносне зоне раздавјања (као нпр. Систем сала). Сви запослени се приликом уласка у Систем салу УЗЗПРО идентификују помоћу ИД картице. Свака ИД картица има одређени ниво приступа. Јасан преглед запослених и њиховог права приступа се води кроз запис ***Контрола приступа***. Запосленима је строго забрањено да своју ИД картицу позајмљују или на било који начин дају на коришћење другој особи, без обзира да ли је она запослена у УЗЗПРО или не. Такође, све апликације су покривене системом сигурносног пријављивања, који представљају предмет контроле приступа.

Поред обавеза које су описане у претходном тексту, обавеза свих запослених је да се придржавају „политике чистог стола и чистог екрана". Запослени су дужни да са својих столова уклоне сву документацију и медије који могу представљати потенцијални ризик од намерног или „случајног" нарушавања интегритета од стране неауторизованих особа. Такође, приступ рачунарима мора бити обезбеђен коришћењем одговарајућих приступних корисничких имена и лозинки, као и активирањем „screen saver"-а који су такође покривени одговарајућим лозинкама. Из претходно наведених разлога, сви посетиоци, али и испоручиоци добара и услуга за потребе УЗЗПРО не смеју се сами кретати кроз радне просторије, већ увек мора постојати одговорна особа из УЗЗПРО-а која ће бити „у пратњи".

Послови физичко-техничке безбедности се планирају и спроводе на начин описан у процедури **ВОЂЕЊЕ ПОСЛОВА ФИЗИЧКО-ТЕХНИЧКОГ ОБЕЗБЕЂЕЊА**. Опрема за гашење пожара је доступна и правилно распоређена по просторијама УЗЗПРО. Опрема се редовно прегледа. Запослени у Одсеку за превентивно техничку заштиту су одговорни за организовање и спровођење основне обуке и провере знања из области заштите од пожара за све запослене у УЗЗПРО. Све ове активности су ближе дефинисане процедуром **ВОЂЕЊЕ ПОСЛОВА ЗАШТИТЕ ОД ПОЖАРА**.

У развоју и изради софтверских решења као интегрални део пројекта укључују се модул корисници система и одговарајући нивои права приступа. Саме кориснике система, као и права приступа систему, одређује одговорно лице из органа за који се ради развој софтверског решења који познаје у детаље све пословне процесе који се аутоматизују у сарадњи са главним пројектантом који ради развој софтверског решења. Тим који ради развој разрађује модул за права приступа у оквиру апликативног решења. Одређује се и креира један „user" – корисник администратор који врши администрацију овог модула која подразумева:

- Унос корисника који раде на систему,
- Доделу права приступа систему или одређеним нивоима у оквиру система,
- Укидање или мењање додељених права приступа,
- Брисање корисника система по налогу одговорног лица корисника система,
- Врши креирање и измену шифарника који се користе у систему.

Права приступа се дефинишу на више нивоа:

1. Први ниво заштите права приступа дефинише се на нивоу корисничког рачунара где се креира име корисника и лозинка према упутству **ФОРМИРАЊЕ ЛОЗИНКИ**.

2. Други ниво заштите и права приступа дефинише се у оквиру софтверског решења у „лог-он" процедури где је дефинисан корисник и лозинка за улазак у апликацију.

3. Трећи ниво заштите и права приступа подацима дефинише се преко улога и

овлашћења додељених кориснику система који има тачно дефинисан подскуп операција које ради.

4. Четврти ниво заштите се дефинише тако да се преко „лог фајлова" чувају име корисника и време логовања на систем.

Права приступа софтверском решењу односно апликацији могу се дефинисати на два начина:

- логовање у апликацију преко Windows аутентификације корисника,
- логовање у апликацију и аутентификација креираних корисника у самом софтерском решењу.

Да би користили Windows аутентификацију користи се дефинисана и креирана Windows доменска инфраструктура у оквиру које се креирају корисничке групе и налози корисника са одређеним правима на систему који се користе у оквиру логовања на апликацију.

У оквиру софтверског решења дефинишу се групе корисника и корисници са одређеним правима на основу којих се врши провера аутентификације.

Права приступа и доступност одређеним подацима у оквиру апликације дефинишу се преко рола-улога корисника на систему.

Сва права додељена су систем администратору пројекта који је суперусер који врши креирање и администрацију свих осталих права и улога корисника. Та права су додељена пројектном тиму који ради развој и одржавање пројекта.

6. **УПУТСТВА** (која произилазе из ове процедуре)

- Упутство **ФОРМИРАЊЕ ЛОЗИНКИ**;

7. **ЗАПИСИ** (који произилазе из ове процедуре)

Назив записа	Број примерака	Период чувања	Одговорност за чување	Прилог број
Захтев за доделу права приступа	1	До укидања права приступа	Начелник одељења за системско-техничку подршку	
Контрола приступа	1	Трајно, ажурира се	Шеф одсека за системску подршку	