ПРОЦЕДУРА

УПРАВЉАЊЕ ПРИСТУПОМ

Израдио: Бобан Цветковић

Контролисао: Петар Јовановић

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: 03.07.2023.

Директор: Дејан Матић

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;
- Управа - Управа за заједничке послове републичких органа;
- Директор Управе – директор Управе 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. Закон о информационој безбедности;
- Закон о информационој безбедности;
- Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја;
- Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја;
- Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја;

❖ Наведени стандарди су били важећи у тренутку проглашења докумената QMC-а. У случају објављивања нових издања, корисници се упућују на коришћење важећих верзија стандарда.

5. ОПИС ПРОЦЕДУРЕ

5.1 Додељивање и укидање права приступа

Уколико постоји потреба да запослени у Управи користи електронску пошту или приступа неком од портала Управе, потребно је да се достави одговарајући формулар попуњен и потписан од стране начелника Одељења у коме запослени ради. У захтеву се наводе подаци о лицу које подноси захтев, као и област за коју се приступ захтева са објективним разлогом потребе за дозволом приступа.

По пријему захтева приступа се обради захтева. Одлуку о додели права приступа доноси директор Управе.

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 Контрола 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 имовини и врше по потреби проширење или смањење тих приступа.

Сви имаоци права приступа (како они „регуларни”, тако и „привилеговани”) могу приступити једино ресурсима за које имају овлашћење да користе, 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 добара и услуга за потребе Управе, приликом запослења и на сваких шест месеци пролазе безбедносну проверу од стране МУП-а и осталих одговарајућих служби како би им се уопште омогућио физички приступ згради у Немањиној 22-26.

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

5.2 Управљање приступом

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

Како би се заштитиле области у којима се налазе осетљиве или критичне информације и опрема, користе се адекватне безбедоносне зоне раздвајања (као нпр. систем сала). Сви запослени се приликом уласка у Систем салу Управе 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 Управи или не. Такође, све апликације су покривене системом сигурносног пријављивања, који представљају предмет контроле приступа.

На сваком рачунару у мрежи инсталиран је Windows Defender антивирусни софтвер. Ажурирање антивирусне заштите као и безбедносних закрпа оперативног система на клијентским рачунарима врши се преко интернет конекције, а то је дужност сваког запосленог који користи рачунар.

Поред свега горе описаног, 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 и испоручиоци добара и услуга за потребе Управе, не смеју се сами кретати кроз радне просторије, већ увек у пратњи имају одговорну особу из Управе.

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 Управе и редовно се 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 Управи. Све ове активности су ближе дефинисане процедуром *Вођење послова заштите од пожара*.

Када је у питању приступ заједничким документима, у зависности од потреба и захтева корисника администратор формира заједничку централну локацију на којој је омогућено креирање и модификовање дељених докумената у облику директоријумске структуре. Строго се води рачуна да се за сваког појединачног корисника одреди минимални ниво приступа дељеним директоријумима и документима неопходан за несметан рад. Администратор дефинише ниво приступа коришћењем дозвола за дељење директоријума и безбедносних дозвола за дељене директоријуме и документе.

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 софтверском 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 улога корисника на систему.

Сва права додељена су систем администратору пројекта који је суперјузер 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	1
Контрола приступа	1	Трајно, ажурира се	Шеф одсека за системску подршку	2

Прилог 1

Управа за заједничке послове републичких органа
Сектор за информатичку подршку
Немањина 22-26, Београд

Телефон: +381 11 363 1916
Факс: +381 11 361 0695
Имејл: informaticka.podrska@uzzpro.gov.rs

ФОРМУЛАР ЗА ЗАДУЖЕЊЕ, ОТВАРАЊЕ НАЛОГА ЕЛЕКТРОНСКЕ ПОШТЕ И ОМОГУЋАВАЊЕ ПРИСТУПА ПОРТАЛУ И АПЛИКАЦИЈАМА УПРАВЕ ЗА ЗАЈЕДНИЧКЕ ПОСЛОВЕ РЕПУБЛИЧКИХ ОРГАНА

Напомена: **Формулар за своје запослене попуњава и прослеђује одговорно лице сектора/одсека.**

ПОДАЦИ О КОРИСНИКУ НАЛОГА

Назив државног органа

Назив Сектора

Назив Одељења

Назив Одсека/Групе

Адреса државног органа

Име и презиме лица на које се задужују налози или технички уређаји

Локација на којој треба поставити налоге или доставити уређаје

(адреса, спрат, крило, канцеларија)

Телефон

Мобилни телефон

Листа онога шта се задужује

- Картица за евиденцију радног времена ☐
- Имејл адреса ☐
- Рачунар ☐
- Сим картица ☐
- Мобилни телефон ☐
- VPN приступ * ☐
- _____ ☐
- _____ ☐
- _____ ☐
- _____ ☐

Уколико је потребан приступ одређеним апликацијама или порталу, уписати називе тих апликација, портал за који се тражи приступ као и тражена права за приступ порталу (администрација, уписивање, читање ...)

*За отварање или продужење VPN налога потребно је попунити и допунски формулар број 2 који је у прилогу

ОДГОВОРНОСТ ДУЖЕЊА НАЛОГА

Подаци о налогу (корисничко име и шифра) представљају поверљиве податке, и корисник је дужан да их третира као такве. За неовлашћено одавање и коришћење ових података у потпуности је одговоран корисник који је дати налог задужио.

Рачунар који се користи за приступ мрежи државних органа мора бити адекватно заштићен одговарајућим антивирус софтвером, који се редовно ажурира, што представља обавезу корисника налога. За било какве упаде и неовлашћене радње извршене преко овог налога одговоран је корисник тог налога.

Овим изјављујем да сносим пуну одговорност за последице до којих може доћи због непоштовања правила, тј. злоупотребе података.

потпис одговорног лица сектора/одсека	лице које задужује налог
_____	_____
име и презиме одговорног лица (штампаним словима, потпис)	име и презиме лица које задужује налог (штампаним словима, потпис)

Прилог 2

Канцеларија за информационе технологије и електронску управу
Влада Републике Србије
Немањина 11, 11000 Београд

Телефон: +381 11 7358-400
Имејл:
it.podrska@ite.gov.rs

ФОРМУЛАР ЗА VPN НАЛОГ

АДМИНИСТРАТИВНИ КОНТАКТ

(Одговорно лице у републичком органу)

Подносилац захтева

Име и презиме

Назив републичког органа

Адреса (улица, број, спрат)

Телефон

Мобилни телефон

Имејл адреса

ЛИЦЕ КОЈЕ ЗАДУЖУЈЕ VPN НАЛОГ

Име и презиме

Назив републичког органа

Адреса (улица, број, спрат)

Телефон

Мобилни телефон

Имејл адреса

VPN налог се региструје или продужава регистрација - (заокружити жељену опцију)

☐ продужава регистрација

Обавезна поља код продужења — URL адреса за конекцију: https://gw.uzzpro.gov.rs/

Username:

☐ креира нов налог

ОПИС ПРИСТУПА

ТРАЖЕНА ПРАВА ПРИСТУПА VPN НАЛОГА

IP адреса сервера / рачунара којој се приступа VPN-ом	Протокол	Порт	Опис приступа

ОДГОВОРНОСТ ДУЖЕЊА НАЛОГА

Подаци о налогу (корисничко име и шифра) представљају поверљиве податке, и корисник је дужан да их третира као такве. За неовлашћено одавање и коришћење ових података у потпуности је одговоран корисник који је дати налог задужио. Рачунар који се користи за приступ мрежи државних органа мора бити адекватно заштићен одговарајућим антивирус софтвером, који се редовно ажурира, што представља обавезу корисника налога. За било какве упаде и неовлашћене радње извршене преко овог налога одговоран је корисник тог налога.

Овим изјављујем да сносим пуну одговорност за последице до којих може доћи због непоштовања правила, тј. злоупотребе података.

отпис одговорног лица у државном органу	лице које задужује налог
_____	_____
име и презиме одговорног лица у државном органу	име и презиме лица које задужује налог
(штампаним словима, потпис)	(штампаним словима, потпис)