- захтјев се похрањује у базу података,
- администратор има могућност прегледа захтјева према критерију,
- администратор је дужан редовно прегледавати захтјеве,
- затварање захтјева има предност над отварањем захтјева.

Протокол комуникације између подносиоца захтјева и одговорне особе, те евиденције самих захтјева може бити реализован и на неки други начин одобрен од стране институције.

**4. Отварање корисничког рачуна**

Кориснички рачун могуће је отворити:
- запосленима,
- трећој страни.

Процедура отварања корисничког рачуна:

**запосленима:**
- овлашћена особа институције путем апликације подноси захтјев за отварање корисничког рачуна новом запосленом,
- администратор система на основу добијених података отвара кориснички рачун.

**трећој страни:**
- за отварање корисничког рачуна трећој страни потребна је сагласност овлашћеног лица (администратор информационог система) институције,
- овлашћено лице је главно и одговорно лице у сарадњи са трећом страном, и као такво има права давања сагласности за отварање корисничких рачуна,
- код отварања корисничког рачуна за трећу страну потребно је одредити временски период колико ће рачун бити активан.

**5. Замрзавање корисничког рачуна**

У случају дужег планираног некоришћења информационог система (нпр. због едукације у иностранству, болести, неплаћено одсуство и сл.) кориснички рачун потребно је замрзнути (преко Active Directory за институције које су кориснице еВладе). Замрзавањем корисничког рачуна избјегавају се непотребни поступци затварања и отварања рачуна, али и спрјечавају безбједносни инциденти који могу настати коришћењем корисничког рачуна од стране других лица док стварни власник није присутан. Замрзавање рачуна одвија се на начин да подаци остану у бази података о кориснику, али се у посебно поље назначи да је рачун замрзнут. Замрзнутом корисничком рачуну није потребно мијењати лозинку у одређеном временском периоду како је дефинисано политиком. Такође се заобилазе све друге безбједносне контроле од стране система за које је потребна интеракција корисника. Замрзнути кориснички рачун могуће је вратити у употребу (одмрзнути) на захтјев корисника и одговорне особе, с тиме да захтјев мора бити документован и одобрен као и код отварања новог захтјева.

**6. Затварање корисничког рачуна**

Затварање корисничког рачуна посебно је осјетљив поступак, а осјетљивост зависи о организацији управљања корисничким рачунима. Што је управљање рачунима неквалитетније изведено, то ће затварање корисничких рачуна бити компликованије. На примјер, ако се кориснички рачуни отварају без документовања и на основу тренутних потреба, након нпр. године дана више се не зна ко има право приступа над којим ресурсима. Тада је и затворити кориснички рачун пуно теже. Уколико "затвореном" кориснику остану нека права приступа, пут за почињење злонамјерних акција му је отворен. Ово је још један примјер зашто је квалитетна организација корисничких рачуна потребна.

Затварање корисничког рачуна одвија се кроз сљедеће фазе:
- при прекиду радног односа потребно је предати захтјев о затварању корисничког рачуна запосленог,
- трећим лицима кориснички рачун се затвара након дефинисаног временског периода приликом отварања рачуна, или уколико је потребно прије на захтјев одговорног лица задуженог за сарадњу са трећом страном,
- лице одговорно за вођење корисничких рачуна дужно је редовно прегледавати запримљене захтјеве за затварањем рачуна те их правовремено затворити,
- уколико постоји потреба, кориснику је могуће пријевремено затворити кориснички рачун без претходног обавјештења на основу писаног захтјева овлашћене особе институције.

**7. ЗАКЉУЧАК**

У складу са Политиком и Смјерницама о корисничким рачунима и правима приступа препоручује се Институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правила/процедуре о корисничким рачунима и правима приступа**.

Литература

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017. – 2022. година ("Службени гласник БиХ", број 38/17)
2. Стандард ИСО/ИЕЦ 27001 – Безбједносне технике – Систем за управљање безбједношћу информацијама – Захтјеви
3. Стандард ИСО/ИЕЦ 27002 – Безбједносне технике – Правило добре праксе за контроле безбједности информација
4. Закон о заштити тајних података ("Службени гласник БиХ", број 54/05 и 12/09)

## СМЈЕРНИЦЕ О БЕЗБЈЕДНОСНИМ КОПИЈАМА

**1. Сврха**

Данас рачунари и апликације служе за повећавање продуктивности, смањивање трошкова и уштеду времена потребног за обављање посла. Уколико се недовољна пажња посвети ризицима који угрожавају рачунарске системе, у институцијама су могуће ситуације које могу узроковати застоје у пословању. Да се не би догодио непланирани застој, институције морају редовно извршавати процедуре за израду и одржавање резервних копија. У противном може доћи до катастрофалних посљедица. Узрок томе је што је пословање зависно у информационим технологијама. Пред информатичке податке се постављају високи критерији заштите који су једнаки или чак већи од критерија заштите записа у пословним књигама. Информациони систем је дио инфраструктуре институције те је из тог разлога недоступност истог или уништење података велики ризик за који треба планирати мјере контроле и обављати поступке којима се повећава потпуно, безбједно и јефтино враћање података.

Израда резервних копија (енг. backup) је основна претпоставка која се поставља пред систем који мора задовољавати резервне захтјеве. Поступак израде резервних копија заједно са поступком повратка података, представља основну процедуру којом се систем штити од губитка података и обезбјеђује брза обнова података у случају

неправилности у раду система као што су нпр. прекиди у раду рачунарског система, инфекције вирусима или пак природне катастрофе попут поплава и пожара. Потребно је испитати исправност резервне копије и процијенити колико је поуздан медиј на којем је она смјештена. Резервна копија губи своју намјену уколико се за вријеме поврата података открије да је она на погрешном медију, погрешно означена или уништена. Резервне копије података, смјештене на информационом систему институција, раде се у сврху обезбјеђења података од виталног значаја за нормално функционисање институције. Задатак резервних копија је обезбједити опоравак система на основи аутентичних, потпуних и расположивих претходно похрањених података, у случају оштећења насталих повредом интегритета података услијед временских непогода, потреса, ратних разарања, пожара, поплаве или хаварије самих система.

Политика резервних копија има намјеру да јединствено у цијелој институцији дефинише начине поступања према подацима, начине израде резервних копија те враћања података у случају одређених губитака. Ризик који се односи према информацијама одређује свака институција засебно, а учесталост извођења израде резервних копија се одређује у складу са важношћу информација и припадајућим ризиком. Поступак израде резервних копија и враћање података треба бити документован у облику процедуре и примјењив у свим дијеловима институције.

**2. Разлози за израду резервних копија**

Један од главних разлога за израду резервних копија је расположивост система. Сваки поремећај у раду система се одражава у престанку рада истог. Посљедице немогућности одвијања пословних процеса се зависно о важности тих процеса, мјере у различитим износима (од хиљаду до милион). С тим разлогом је потребно обезбједити израду резервних копија како би се у ванредним околностима могло наставити са пословањем. Обезбјеђење непрекинуте расположивости и могућност наставка рада информационог система услијед непредвиђених околности, чине успјешним пословање институције, док се у случајевима неиспуњена тих услова узрокују уз финансијске и неке непоправљиве штете као што су губитак угледа, неповјерење грађана и престанак сарадње са међународним институцијама. Уколико институција располаже резервним копијама, у случајевима елементарних непогода (пожар, потрес, поплава, саботаже, терористички напади, итд…) или других узрока прекидања рада, институција посједује могућност успостављања пословања на другим локацијима. Неки од узрока који могу проузроковати прекид пословања су кварови на струјном напајању, кварови рачунара или дисковних медија чиме се тренутно губе информације. Осим тих узрока прекидања пословања постоје и они узроковане људским фактором, а то су људска погрешке, злонамјерне активности локалних корисника или удаљених нападача. Такође, вируси и други малициозни програми могу уништити вриједне податке. Још један разлог за израду резервних копија је законска обвеза чувања финансијских и других сличних података. Зависно о прописаним роковима за чување одређених података дефинише се и политика израде резервних копија. Резервне копије су такође валидан доказ у судским процесима и зато је понекад важно посједовати периодичне резервне копије којима се може доказати постојање одређених информација. Институције често требају чувати старе податке када раде на пословима који укључују истраживање и развој. Наиме, током развоја неког програма или сл., који може трајати и више мјесеци или година, могуће су ситуације у којима је потребно одустати од одабраног смјера рада и вратити се у неку стару фазу која може бити уназад и неколико мјесеци.

**3. Поступци у изради резервних копија**

Сваки институција сам за себе треба донијети одлуку о томе који су им подаци важни и за које податке је потребно израђивати резервне копије. У пракси се обично израђују резервне копије података генерисаних апликацијама док се за саме апликације у правилу не израђују резервне копије. Приликом процеса израде резервних копија пажњу је потребно посветити и смјештају података. Наиме, подаци се могу спремати на локалном рачунару, на удаљеном рачунару који служи као "дата" сервер или на неким преносним медијима. Сам процес израде резервних копија одвија се у неколико фаза:

**Идентификација података**

Институције требају одлучити који подаци су важни за институцију или кориснике. У пракси се као најбоља пракса показала симулација којом се дефинишу подаци које је потребно вратити у случају квара рачунара. Обично су то подаци које генеришу текстуални и табеларни програми, базе података и електронска пошта. Многи од њих посједују могућност стварања јединствене backup датотеке из које је накнадно могуће вратити податке. Свакако је добро посавјетовати се са стручњацима приликом одлучивања о томе што све је потребно ставити у безбједносну копију.

**Одређивање прихватљивог медија**

С обзиром на природу садржаја чија резервна копија се креира, потребно је одредити и прикладан медиј. Најчешће се одабире онај медиј који је на једноставан начин подржан од рачунара, што значи да спремање текстуалних датотека у облику исписаних страница није најприступачнији облик. Такође Институција може да ради бекап на више од једног медаја ради повећања редундандности наведених бекапа.

**Означавање резервних копија**

Сви медији који садрже резервне копије морају бити јединствено и прецизно означени. Информације које су истакнуте означавају датум стварања копије, број копије у низу копија и датум стварања. Препоручује се одржавање записа о резервним копијама у писаном облику гдје су наведене детаљније информације и референце. Такође у случају коришћења софтвера за креирање аутоматског бекапа препуручује се да исти генерише наведене податке о датуму броју резервне копије у електронском облику.

**Чување резервних копија**

Записе о резервним копијама потребно је одређено вријеме чувати. У пракси се користе записи стари један дан, седмични, мјесечни, полумјесечни, полугодишњи и годишњи – зависно о томе која је количина података коју желимо сачувати. Овим поступком се институције обезбјеђују од губитка података и поступак је за кориснике потпуно транспарентан. Сам поступак се у пракси најчешће назива "генерацијска резервна копија" која може садржавати и по неколико генерација записа резервних копија.

**Смјештај резервних копија**

Резервне копије се требају смјестити заједно са припадајућим записима на безбједну локацију. У идеалној ситуацији се копије држе на другој локацији довољно удаљеној од оригиналне како би се избјегле природне непогоде (ватра, поплава, …) и тиме омогућило безбједно враћање података и одвијање процеса пословања.

**Тестирање резервних копија**

Након обављања процеса израде резервних копија потребно је тестирати враћање података с медија. Овим поступком се провјерава да ли су сви подаци из резервне копије исправно враћени. Тиме се обезбјеђује процес евентуалног враћања података у случају неке опасности. Институције увијек морају посједовати план за најгори могући сценариј као што је нпр. потпуни губитак података на систему. Због тога треба постојати дефинисан поступак враћања података на замијењени хардвер и успостава претходног оперативног стања. Након обављене процедуре враћања података често је потребно обновити лиценце за припадајуће апликације јер су поступци којима се генерише лозинка често везани уз конфигурацију хардвера на рачунару као што је чврсти диск, MAC адреса мрежне картице или име сервера. Поступак тестирања враћања података могуће је извршити у двије фазе:

- тестирање на постојећем рачунару или
- тестирање на рачунару сличне конфигурације.

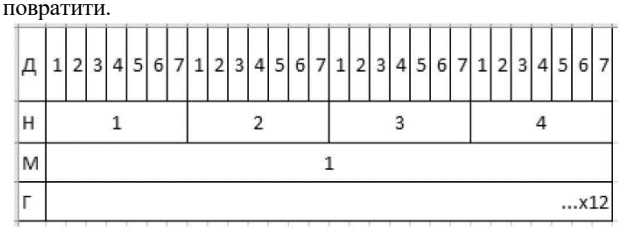
У поступцима израде резервних копија потребно је обратити пажњу на додатне захтјеве. Важно је гдје су подаци смјештени с обзиром на природу података и њихову важност за Институцију. С обзиром на постојеће законе о чувању података, уколико се ради о финансијским подацима или слично, потребно је чувати копије одређени број година. Уколико се при коришћењу апликација ради о уговорима о коришћењу у одређеном периоду, потребно је обезбједити уништење података након истека истог уговора. При изради резервних копија добро је имати овакву листу за провјеру:

- да ли су израђене резервне копије свих података, оперативног система и помоћних програма адекватно и систематски,
- постоје ли записи о садржају резервних копија и њиховом смјештају,
- постоје ли записи о лиценцираним апликацијама,
- постоје ли копије медија или записа спремљене на удаљеној локацији,
- да ли је повремено проведен поступак враћања података са медија,
- може ли нови хардвер читати податке са постојећих медија,
- хоће ли се због постојећих лиценци апликација покретати на новом хардверу и
- да ли је проведен поступак потпуног враћања података у одређеном временском периоду.

У пракси се не препоручује коришћење само једног медија за потребе архивирања. Ризик који је повезан са губитком података је мањи уколико постоји више копија истих података. Уколико се ради о оптичким медијима препоручује се коришћење већег броја јер је њихова цијена занемарива са обзиром на штету која се може проузроковати губитком података. Такође, уколико се свакодневно проводи израда резервних копија или барем у неким дефинисаним периодима, смањује се ризик губитка података. Уколико се периодично проводи стварање резервних копија увијек постоји могућност враћања података. А у случајевима када се ради о већем квару као што је нпр. механички квар на тврдом диску, онда су најчешће уништени сви подаци на њему. Једини начин враћања података је из резервне копије. Препоручује се користити други медиј од оног изворног на којем су подаци из којих су израђене резервне копије. Постоји више метода за стварање резервних копија. Једна од најчешћих је стварање властитих архива од стране Институције. При томе се најчешће израђују резервне копије за оне податке које Институцији представљају важан информациони ресурс. Осим таквих стварања архива одређених специфичних информација, често се користи и стварање резервних копија система база података. Администратори у пракси проводе стварање резервних копија низа корисничких директорија. При томе администратори могу радити резервне копије свих података или само измијењених тј. нових података. Пошто се код израде резервне копија најчешће користе велике количине датотека, у правилу се оне компресују одговарајућим системским алатима.

**4. Врсте резервних копија**

Стварање резервне копије (backup) не утиче на степен безбједности самог ИС, али је од кључног значаја када се послије резервне кризе јави потреба да се изгубљени подаци поврате. Понекад је на основу резервне копије могуће утврдити узрок пада система – реконструкцијом резервних пропуста или грешака у ИС, и слично. Препоручено је и екстерно и интерно чување копија. Екстерни backup се односи на чување датих копија података на посебним дисковима у посебним сефовима који су заштићени од могућих незгода (примјер: ватростални сефови). Интерни бацкуп подразумјева чување копија базе података у оквиру ИС, односно на различитим серверима или на серверу који је посебно намјењен за backup. Сервере треба копирати ноћу. Диференцијална копирања (backup промјена) треба обављати сваке ноћи, док цјелокупни бацкуп треба обављати једном у седам дана. Дневне израде копије треба чувати једну седмицу, док би седмични требало чувати један мјесец. Мјесечне резервне копије треба чувати једну годину, док би годишње требало чувати заувијек. Подразумијева се да те резервне копије треба заштити од свих врста физичких повреда. Треба имати у виду да се избрисани подаци понекад не могу повратити.




| Ознака | Опис | Период чувања |
|---|---|---|
| Д | Дневни *backup* | 7 дана |
| Н | Недељни *backup* | 1 мјесец |
| М | Мјесечни *backup* | 1 година |

У наставку слиједе препоруке из праксе за израду резервних копија:

- Провјера враћања података након неправилности у раду система - у пракси се обављају провјере и тестирања да ли је могуће наставити пословање нпр. након квара на чврстом диску, уколико смо изгубили медије са резервним копијама или су оне украдене. У тестирање су укључене различите смјернице које анализирају колико је потребно да се пословање врати у фазу кад су изгубљени подаци, који су предуслови потребни за то, ко је одговоран и сл. Све ове смјернице морају бити садржане приликом израде политике резервних копија.
- Периодична провјера резервних копија - из разлога што медији и припадајући хардвер могу бити веома

непоуздани потребно је периодички проводити тестирања која се односе на њихову исправност. Велика количина података похрањених на тракама или дискетама је бескорисна уколико се не могу прочитати са истих. У ту сврху потребно је периодично провјеравати исправност резервних копија.

- Чување старих верзија резервних копија - некад је потребно извјесно вријеме како би се утврдило да је нека датотека уништена или побрисана. Због таквих случајева увијек је потребно чувати старе верзије резервних копија одређено вријеме или онолико колико налаже закон. Могуће је чувати седмичне, мјесечне, полугодишње или годишње верзије резервних копија. Препоручује се старе копије чувати на различитој локацији од оне на којој су подаци.
- Провјера система база података прије израде резервних копија - уколико се ради о повратку података система који је претходно уништен онда је резервна копија бескорисна. Препоручује се прије израде резервне копије провјеравање интегритета система база података.
- Провјера да се датотека не користи током стварања резервног записа - уколико се датотека користи приликом израде резервне копије она је бескорисна јер не садржи исправну и важећу верзију.
- Стварање резервне копије прије великих промјена у систему база података - корисно је имати резервну копију прије тестирања новог хардвера, поправака на систему или инсталације нових апликација.

Приликом израде резервних копија институције могу користитит и друге методе као што су electronic vaulting, journaling i mirroring у зависности о врсте пословавања и потреба институције када је у питању израда резервних копија.

**5. Закључак**

Процесом стварања сигурносних копија и повратом података смањују се ризици којима је изложен информацијски сустав. Редован и поуздан поступак израде сигурносних копија је поступак који се не смије избјећи. Без обзира како се третира сустав не могу се избјећи ризици од нежељених посљедица. Ризици су обично већи него су људи то способни схватити, а према подацима се треба односити озбиљно прије него се осјете посљедице губљења истих. По статистици 90% организација пропада ако изгубе виталне записе што показује колико су модерне организације овисне о информацијској подршци. Један од недостатака израде сигурносних копија је цијена. Наиме, процес укључује одговарајуће медије, опрему на којој се похрањују информације, запослените који су задужени за одржавање сигурносних копија и примјену политике израде сигурносних копија, а то организацијама узрокује трошкове без јасно видљивих резултата. Ипак, дугорочно гледано та цијена је занемарива у односу на цијену коју може платити тврткa или појединац уколико није у стању обављати посао. Додатан проблем који је могућ код организација које проводе политику израде сигурносних копија је отпор запосленика. Запослени често сам поступак израде сигурносних копија сматрају беспотребним јер нису свјесни важности сигурносних копија за цијелу организацију. Ипак сви су ови потенцијални недостаци израде сигурносних копија занемариви у односу на могућност прекида пословања и пропадања организације у случају изостанка података. Стога је податке потребно адекватно заштити, а један од неопходних начина је и израдом сигурносних копија.

У складу са Политиком и Смјерницама о резервним копијама препоручује се Институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правила/процедуре за израду резервних копија.**

Литература

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017. – 2022. година ("Службени гласник БиХ", број 38/17)
2. Стандард ISO/IEC 27001 – Безбједносне технике – Систем за управљање безбједношћу информацијама – Захтјеви
3. Стандард ISO/IEC 27002 – Безбједносне технике – Правило добре праксе за контроле безбједности информација

## СМЈЕРНИЦЕ
## О ЗАПОСЛЕЊУ И ПРЕКИДУ ЗАПОСЛЕЊА

**1. Сврха**

Сврха смјерница о запослењу и прекиду запослења је дефинисати процедуре којима ће се прецизирати кораци које је потребно предузети у погледу безбједности приликом запослења, склапања уговора о запослењу или сарадњи и које дефинишу на који начин квалитетно провести прекид запослења или раскид уговора. Циљ наведених процедура је смањење ризика од људске погрешке, крађа, превара и злоупотребе ресурса информационих система институције.

**2. Процедуре склапања уговора**

Одговорна лица при склапању уговора о запослењу или сарадњи требало би да проведу мјере дефинисане сљедећим процедурама:

**2.1. Провјера**

Провјера (енг. screening) у сврху контроле потенцијалних запосленика или пословних партнера једна је од превентивних метода којима институција може дјеловати на безбједност информационог система. Одговорно лице треба провести или иницирати провјеру и испитивање над потенцијалним запосленником. Процес провјере и испитивања треба узети у обзир сва права и законске одредбе приватности те уколико је допуштено укључити сљедеће:

- расположиве референце карактера, пословања итд.,
- преглед доступних ЦВ-а, контрола достављених података,
- потврде о школовању и професионалним квалификацијама,
- докази идентитета (пасош),
- да ли је особа казнено гоњена итд.

Прикупљене податке потребно је документовати као **повјерљиве податке** те према њима направити процјену да ли постоји могућност злоупотребе информационог система од стране потенцијалног запосленика.

**2.2. Услови запослења и уговор одговорности**

Прије запослења особа у институцијама БиХ, склапања партнерства са другом организацијом или укључивања у посао треће стране неопходно је у рјешење или уговор укључити дио који све стране обавезује на придржавање правила дефинисаних безбједносном политиком. Рјешење или уговор треба садржавати додатак са појашњењима и ставовима:

- да сваки запосленик, партнер или трећа страна, прије добивања права приступа имовини организације, треба потписати уговор о повјерењу,