РЕПУБЛИКА МАКЕДОНИЈА
Министерство за информатичко општество и администрација

Информација за ИТ стандарди во државните институции

Скопје, 14.10.2011

Информација за ИТ стандарди во државните институции

Вовед

Информацискатa безбедност (систем на мерки за заштита на информациските системи, посебната телекомуникациска мрежа, документите во електронска форма и податоците во електронска форма од неовластен и случаен пристап, искористување, промена, спречување на пристапот до документите и податоците или нивно уништување, спречување на давањето на административни услуги по електронски пат.

Овој материјал е подготвен согласно Годишната програма за работа на Министерството за информатичко општество и администрација и има за цел зголемување на безбедноста и сигурноста на ИКТ системите, користење на мерки и процедури за заштита и развој на ИТ системите во државните институции. Информацијата содржи: препораки за физичка сигурност/безбедност на капацитети за процесирање на податоци, процедура за управување со резервни копии на податоци (back up), процедура за управување со промени на информациски системи, процедура за управување со сигурносни инциденти, и политика за употреба и сигурност на лозинки.

Потребно е да се има во предвид ризиците во однос на реализацијана препораките кои се: недостаток на капацитет и обучени лица за имплементација на мерките и препораките, неадаптирање кон новите трендови т.е. отпорност кон промени, несоодветното ниво на поставените стандарди.

Во продолжение накратко се објаснети целите на гореспоменатите препораки, процедури и политики. Препораките, процедурите и политиките за заштита и развој на ИТ капацитети детално се објаснети во продолженитето на текстот на оваа Информација.

Препораките, процедурите и политиките ќе допринесат кон зголемување на информацискатa безбедност.

I. Процедура за управување со резервни копии на податоци (back-up)

Намената на овој документ е прецизно да ги дефинира активностите кои треба да бидат преземени со цел на успешно управување со архивите на податоци во организацијата.

При подготовката на резервни копии на системи и податоци, детални упатства за архивирање и избор на системи за архивирање, потребно е квалитетот на истите да се одржи со примената на следните фактори:

- *Перзистентност* е мерка за тоа со колкава релативна фреквенција на појава на грешки (рата на грешка) медиумот ги запишува/чува податоците. Основната

рата на грешка може да биде подобрена со креирање на повеќе од една копија со чување на копии на повеќе локации, со ротација на медиуми и со контрола на условите во околината на чување.

- *Грануларност* е фреквенцијата со која се прават резервни документи. Систем за кој се прават дневни резервни копии е по ажурен отколку систем со седмични резервни копии.
- *Траење* е должината во временски единици на чување на резервните копии, односно времето после промена кое овозможува истата да биде вратена во случај на потреба.

II. Препораки за физичка сигурност / безбедност на капацитети за процесирање на податоци

Целта на физичката сигурност е заштита на доверливоста, интегритетот и достапноста на податоците и операциите од загрозување на истите преку физички средства.

Доверливоста на податоците и операциите се штити со превенција на неавторизиран пристап кон опремата (сервери и каблирање) на која се чуваат, пренесуваат и обработуваат податоците.

Интегритетот и достапноста на податоците и операциите се штитат со превенција на неавторизиран пристап кон опремата (сервери и каблирање) на која се чуваат и обработуваат податоците како и превенција на прекините на сервисите кои ги дава ИТ, а кои можат да настанат поради човечка грешка, од инфраструктурна природа (на пр.: прекин на електрична енергија) или природна катастрофа.

III. Процедура за управување со сигурносни инциденти

Процедурата за управување со сигурносни инциденти има за цел да ги дефинира процесите, постапките и одговорностите за управување со сигурносните инциденти во информациониот систем на организацијата и известување кон раководството за постојните ризици.

Целта на овој документ е дефинирање и воспоставување на процес за брз и ефективен одговор на сигурносните настани, нивна ескалација, закрепнување од сигурносни настани и известување за сигурносните настани.

Со соодветна постапка на проценка на ризиците, нивно управување и планирање на одговорот на инцидентите се зголемува и способноста на организацијата успешно и брзо да одговори на инцидентите, да ги ограничи и да ги исправи настанатите штетни ефекти, како и да ги намали штетните последици на инцидентите во иднина.

Претпоставка за успешно планирање на одговорот на инцидентите е добро познавање на опкружувањето на информацискиот систем, познавање и следење на

потенцијални закани, од една страна, и познавање на ранливите точки на системот од друга страна.

IV. Процедура за управување со промени во информациските системи

Со оваа процедура прецизно се дефинира постапката за предлагање на промени, разгледување на предлози и донесување на одлуки за реализација на промените со цел подигање на квалитетот на работата на вработените и системите кои се користат во организацијата.

V. Политика за употреба и сигурност на лозинки

Целта на овој документ е формално да дефинира политика во организацијата која се однесува на употребата и сигурноста на лозинките. Потребно е сите вработени да бидат запознаени со истата и да се придржуваат до упатствата изнесени подолу.

* *
*

Препораките, процедурите и политиките за заштита и развој на ИТ капацитети детално се објаснети во продолжението на текстот на оваа Информација.

I. Процедура за управување со резервни копии на податоци (back-up)

1. ЦЕЛ

Намената на овој документ е прецизно да ги дефинира активностите кои треба да бидат преземени со цел на успешно управување со резервните копии на податоци во организацијата.

При подготовката на резервни копии на системи и податоци, детални упатства за архивирање и избор на системи за архивирање, потребно е квалитетот на истите да се одржи со примената на следните фактори:

- *Перзистентност* е мерка за тоа со колкава релативна фреквенција на појава на грешки (рата на грешка) медиумот ги запишува/чува податоците. Основната рата на грешка може да биде подобрена со креирање на повеќе од една копија со чување на копии на повеќе локации, со ротација на медиуми и со контрола на условите во околината на чување.
- *Грануларност* е фреквенцијата со која се прават резервни копии на документи. Систем за кој се прават дневни резервни копии е по ажурен отколку систем со седмични резервни копии.
- *Траење* е должината во временски единици на чување на резервните копии, односно времето после промена кое овозможува истата да биде вратена во случај на потреба.

2. ОБЛАСТ НА ПРИМЕНА

Овој документ е применлив во активностите на Секторот за ИТ во организацијата.

3. РЕФЕРЕНТНИ ДОКУМЕНТИ

- Технолошки упатства за работа со апликации
- Планови на дневни и периодични обработки (за секоја од наведените периодичности во точка 5.1)
- Стандарди – (називи/конвенции) во Секторот за ИТ
- Упатство за работа во систем сала

4. ДЕФИНИЦИИ, ОЗНАКИ И КРАТЕНКИ

Архивирање (анг. Back-up) – подразбира креирање на дупликат на одредени податоци на соодветен медиум за дефиниран временски период.

5. ОПИС

5.1 Општи упатства

- По наводите во оваа процедура потребно е да се развијат посебни упатства за backup/recovery на сите критични системи (и истите заедно со оваа процедура да станат дел од Планот за закрепнување од катастрофа).
- Оваа процедура како и поединечните упатства потребно е целосно да се тестираат/ревидираат најмалку еднаш годишно. Ревидирање на процедурата и тестирање на поединечните упатства е задолжително после значајни промени во системите/апликациите. Потврда на валидноста на тестот прави Директорот на Секторот за ИТ.
- Потребно е да се дефинираат прагови на слободен дисков простор на системите и редовно да се прави проверка на расположливоста на простор кај критичните системи.
- Backup медиумите, медиумите за инсталација (CD, DVD, ...), документираните процедури и упатства мора да бидат сместени на секундарна локација со висока физичка заштита.
- Сценаријата за архивирање мора да бидат планирани и дискутирани на почеток на секој нов ИТ/ИС проект и истите да се ревидираат еднаш годишно.
- На одговорните лица мора да им бидат достапни алатки/процедури/упатства за комплетирање на резервните копии.
- Потребно е одговорните лица да бидат запознаени со локациите каде се наоѓаат медиумите за backup и каде истите се сместуваат по завршетокот на процесот на архивирање.
- За пристап кон резервни копии потребено е одобрување од раководството (Директорот на секторот за информатика или Директорот на секторот сопственик на апликацијата/податоците чии резервни копии се во прашање). Листите за пристап треба редовно да се ревидираат.

5.2 Периодичност на архивирање

Динамика на архивирањето на податоците во организацијата е поделена на:

5.2.1 дневно (се архивира продукциска околина: бази на податоци, системски логови, ...)

5.2.2 периодично

- седмично (бази на податоци, избрани дискови/фолдери, периодични обработки во апликации)
- полумесечно (периодични обработки во апликации)
- месечно (периодични обработки во апликации)
- квартално (периодични обработки во апликации)
- полугодишно (периодични обработки во апликации)

- годишно (периодични обработки во апликации)

5.2.3 вонредно

- повремено (обработки/податоци кои немаат дефинирана периодика)
- интервентно (акции над ресурси кои не се опфатени со стандарди)
- на барање (од одговорни раководни лица или проектанти)

5.3 Содржина на архивата

Архивите на податоци се однесуваат на следните околини:

- продукциска околина
- тестна околина
- инфраструктура (системска околина)

Содржината на фајловите/табелите кои се архивираат треба да опфаќа:

- бази на податоци (со матични податоци за корисниците, шифрарници, извештаи од обработка на надворешни и внатрешни корисници, табели, рекапитулации, прегледи, спецификации, изводи итн.)
- апликативен софтвер (изворен код на програмите и извршни модули на програмите)
- упатства, регистри, процедури за апликациите
- системски софтвер
- поединечни библиотеки/програми на компјутерите на вработените поврзани со работата
- документација

5.4 Постапка на архивирање

Постапката се извршува согласно со упатствата за архивирање на базите на податоци, оперативниот систем и конфигурациите на комуникациските уреди наведени во листата на прилози (подоле во тектот во точка 7.)

5.5 Медиуми за обезбедување на податоците

Во зависности од периодичноста и барањата за архивирање, се користат следните медиуми:

5.5.1 фиксни дискови со капацитет од ... GB

- за вонредни/интервентни архивирања
- за дневни архивирања на барање

5.5.2 магнетне ленти – касети со капацитет од ... GB

- за архивирање на ...

Уреди кои вршат запис на архивираниот материјал:

5.5.3 tape drive – модел 1...

- за магнетни ленти ...

tape drive – модел 2...

- за магнетни ленти ...

5.6 Стандарди за означување на медиумите за архивирање

Медиумите за архивирање се означуваат со етикети како што е наведено подолу::

APPL-XX-YY-ZZ

Легенда:

APPL – кратенка за апликацијата/базата на податоци/системот/уредот

XX - тип на архивирање

DB – база на податоци

OS – оперативен систем

NE – комуникациски уред

YY – периодичност

DN - дневно

7D - седмично

15 - полумесечно

ME - месечно

QU - квартално

6M - полугодишно

GO - годишно

ZZ - тип на фајлови

PE - постојани

TE - повремени

Лабелите за повремени, интервентни и архивирања на барање се формираат на следниот начин:

BKP-EXyymmdd-APPL-YY-ZZ

BKP - backup (архива)

EX - expires (истекува)

yymmdd - година, месец, ден

APPL - скратеница на апликацијата/базата на податоци/системот/уредот

YY - периодичност

ZZ - тип на фајл

Постојат и архиви кои не се во рамки на наведените стандарди и истите се дефинирани со технолошките упатства на поединечни апликации, или на барање на одговорни лица.

5.7 Периодичност на проверка на читливоста на медиумите

Читливоста на медиумите се проверува според следните стандарди:

- дневна архива – случаен примерок од 3 ленти еднаш во 2 месеци
- седмична архива – случаен примерок од 3 ленти еднаш во 6 месеци
- полумесечна архива – случаен примерок од 3 ленти еднаш во 6 месеци
- месечна архива – случаен примерок од 3 ленти еднаш годишно
- квартална архива – случаен примерок од 1 лента еднаш годишно
- полугодишна архива – случаен примерок од 1 лента еднаш годишно
- годишна архива – случаен примерок од 2 ленти еднаш на 3 години

5.8 Периодичност на чување

Резервните копии се чуваат според следните правила:

5.8.1 дневно – 30 генерации

5.8.2 периодично

- неделно – 4 генерации
- полумесечно – 2 генерации
- месечно – 12 генерации
- квартално – 4 генерации
- полугодишно – 2 генерации
- годишно – 10 генерации

Постојат и архиви кои не се во рамки на наведените стандарди и истите се дефинирани со технолошките упатства на поединечни апликации, или на барање на одговорни лица.

5.8.3 вонредно

Иницијаторот на акцијата за вонредните архиви во договор со одговорно лице од Секторот за ИТ одредува колку генерации и/или до кој датум се чуваат архивите.

5.9 Физичко сместување/чување на медиумите

Места за чување на медиумите се:

- фиксни дискови – се наоѓаат во систем сала
- магнетни ленти – се наоѓаат во посебно проектирани шкафови за оваа врста на медиуми, пропишано оддалечени од фиксните дискови и други електро-уреди и машини
- магнетни ленти - дислоцирани копии, се пакуваат во посебно наменети кутии и се сместуваат во просториите на издвоена локација кои се соодветно климатизирани и оспособени.

5.10 Заштита на архивираниот материјал

Архивираниот материјал има неколку видови на заштита:

- физичка заштита
    - место на чување – систем сала, повеќекратно обезбедена:
        - контрола на влез во организацијата
        - авторизиран пристап (магнетни картици)
        - контрола на влез во систем салата од страна на одговорното лице
        - повеќекратна контрола на електро-инсталациите
        - противпожарна заштита

- процедурална заштита
    - стандарди и процедури за:
        - формирање на називите на лабелите,
        - редоследот и начинот на архивирање,
        - манипулација со наведениот материјал,
        - пристапот кон архивите му е дозволен на ограничен број одговорни лица

- дислокација на сигурносните резервните копии на секундарна локација

5.11 Враќање (Restore) на архивираните податоци

Постапката се извршува согласно со упатствата за враќање на архивираните податоци од базите на податоци, оперативните системи и конфигурациите на комуникациските уреди наведени во листата на прилози (подоле во тектот во точка 7.)

6. ОДГОВОРНОСТ И ОВЛАСТУВАЊА

Кон овој документ мора да се придржуваат сите учесници во процесот на архивирање на податоците како и сите останати корисници на податоците.

- Раководството е одговорно за:
    - обезбедување ресурси за имплементација и надградба на системите за архивирање

- Секторот за ИТ е одговорен за:
    - администрација на системот за архивирање
    - редовен надзор на состојбата и исправноста на постојните архиви

- Вработените се одговорни за:
    - Почитување на оваа процедура, чување на важни информации во личните фолдери сместени на фајл-сервер
    - Внимателно чување и спречување на губење на податоци

Ако начинот на задавање на задачите дефинирани во овој документ не е експлицитно дефиниран, тогаш се подразбира еден од следните начини на задавање задачи:

- во пишана форма

- преку електронска пошта

За контролата дали се постапува според овој документ овластен е _____ (Директорот на секторот за информатика)

7. ПРЕГЛЕД НА ЗАПИСИ И ПРИЛОЗИ

Број		Ознака на образецот (број на	Назив на записот	Чување		
				Место	Начин	Време
1.	*1.*		Упатство за изработка на backup/restore на база на податоци за системот Е-набавки	Архива на Секторот за информатика	Регистер / Back-up медиум	3 год
2.	*2.*		Упатство за изработка на backup/restore на web фолдери за системот Е-набавки	Архива на Секторот за информатика	Регистер / Back-up медиум	3 год
3.	3.		...	Архива на Секторот за информатика	Регистер / Back-up медиум	3 год

II Препораки за физичка сигурност / безбедност на капацитети за процесирање на податоци

Целта на физичката сигурност е заштита на доверливоста, интегритетот и достапноста на податоците и операциите од загрозување на истите преку физички средства.

Доверливоста на податоците и операциите се штити со превенција на неавторизиран пристап кон опремата (сервери и каблирање) на која се чуваат, пренесуваат и обработуваат податоците.

Интегритетот и достапноста на податоците и операциите се штитат со превенција на неавторизиран пристап кон опремата (сервери и каблирање) на која се чуваат и обработуваат податоците како и превенција на прекините на сервисите кои ги дава ИТ, а кои можат да настанат поради човечка грешка, од инфраструктурна природа (на пр.: прекин на електрична енергија) или природна катастрофа.

1. Изложеност на ризик

При случајно или намерно непочитување или неимплементирање на контролите за физички пристап кон сервер салата/податочниот центар, организацијата е изложена на следните ризици:

- Неовластен влез
- Оштетување, вандализам или кражба на опрема и/или документи
- Копирање или преглед на осетливи или информации со авторски права
- Менување на осетлива опрема или информации
- Јавно објавување на осетливи информации
- Злоупотреба на ресурсите за обработка на податоци
- Уцена
- Проневера

Од перспектива на информациските системи, уредите/поставките/објектите на кои им треба физичка заштита ги вклучуваат следниве:

- Сервер сала
- Простории каде се програмира
- Операторски конзоли и терминали
- Библиотеки со ленти, дискови и останати магнетни/оптички медиуми
- Простории за чување на опрема и залихи

- Простории каде се чуваат backup (резервни) копии надвор од примарната локација
- Контролна соба за влез и излез
- Плакари со комуникациска опрема
- Телекомуникациска опрема (вклучително радио опрема, сателитски кабли, модеми и надворешни мрежни конекции)
- Персонални компјутери
- Главни извори на струја
- Места за технички/хардверски отпад
- Дедицирани телефони / телефонски линии
- Портабилна опрема (рачни скенери и уреди за кодирање, баркод читачи, лаптопи, важни принтери и др.)
- Документацијата за системите, инфраструктурата и апликациите

2. Трендови

Одредени современи трендови поврзани со податочните центри за обработка и чување на податоци се причина за подобрување и менување на аспектите на физичката сигурност. Меѓу другото за тоа придонесуваат и:

- Консолидација (обединување) на податочните центри: Обединувањето на податочните центри обезбедува многу погодности при управувањето со физичката безбедност бидејќи се намалува бројот на локации за заштита. Сепак, обединувањето значително ја зголемува вредноста на средствата содржани во централниот податочен центар отколку кога тие средства се распространети по поодделните центри и истовремено го зголемува ризикот на постоење на ‘единствена точка на пад’(‘single points of failure’) кое од своја страна ја налага потребата за пософистицирани мерки на сигурност за адекватно справување на зголемениот ризик.
- Outsourcing на услуги: Outsourcing-от на услуги (вклучувајќи ја и физичката и логичката сигурност) може да доведе до зголемена фреквенција на напуштање и доаѓање на персонал, намалена можност за увид во генералните операции и помала комуникација и соработка помеѓу одделенијата задолжени за физичка и ИТ безбедност
- Зголемената важност на закрепнување од катастрофа: Зголеменото значење на ‘disaster recovery’ налага постоење на секундарната локација која ќе биде обезбедена на сличен начин како и примарната локација/сервер сала. За време на катастрофа важно е да се одржи физичката безбедност на персоналот и податоците во тек на преселбата кон секундарната локација.

3. Препораки

Препораките за физичка сигурност се категоризираат како “традиционален пристап” но вредноста од нивната имплементација е актуелна и не помалку

значајна и во современи услови. За зголемена сигурност и потемелно обезбедување препорачливо е да се имплементира стратегијата на 'длабинска заштита' ('defense-in-depth'). Пристапот со 'длабинска заштита' значи имплементација на повеќе, различни по природа контроли за заштита од одреден напад врз ранливите точки. За обезбедување на повеќеслојна заштита овој принцип треба да се примени на следниве секции:

- Локација

- Сервер салата треба да се наоѓа во дедицирана зграда, на растојание од најмалку 30-тина метри од главната улица/пат; ако е утврдено дека зградата е подложна на земјотреси потребна е имплементација на соодветни стандарди за сеизмичка околина;
- Податочниот центар/сервер салата треба да бидат скоро незабележливи (т.е. не треба да се стават показатели и знаци кои го означуваат постоењето на сервер салата и дека во зградата се наоѓа податочен центар).
- Сервер салата треба да биде лоцирана подалеку од извори на електромагнетна интерференција или интерференција на радио бранови (вакви извори има кај телекомуникациски станици и сл.)
- Потребно е сервер салата да биде изолирана од контаминирачки влијанија на простории за печатење (print rooms), машински работилници, кујни или било кој друг фактор со високо ниво на контаминација или активност. Влезовите во филтрите од клима-уредите во сервер салата не траба да бидат во близина на издувни цевки од генератори или други извори.
- Потребно е да се избегне, каде што е можно, хардверот да се лоцира под област каде има опасност за протекување на вода или други течности. Дополнителна заштита се постигнува со тоа што цевките од клима-уредите не се спроведуваат низ таванскипразнини во сервер салата. Ако сервер салата се лоцира ниско или под нивото на зградата постои ризик за потенцијално протекување од надворешноста.
- Сервер салата треба да биде лоцирана на место кое нуди потенцијал за идно проширување. Иако промените и напредокот во технологијата одат во насока на тоа хардверот да е се поефикасен во единица простор, потребно е да се предвиди простор за проширување во случај на раст и експанзија на сервер салата.

- Конструкција на зградата

- Просториите од сервер салата не треба да имаат прозорци кои гледаат кон надвор, со исклучок на посебно преградени делови кои не содржат податоци или опрема и кои се одделени од остатокот на сервер салата со точка на проверка на сигурност (на пр.: чуварска служба, дупла врата со контрола на пристап).
- Надворешните ѕидови треба да бидат направени од цврст бетон со најмалку 30-тина cm дебелина

- Конструкција на подот

- Подигнатиот под нуди флексибилност при поставувањето на кабли, лоцирањето на хардверот и климатизацијата на просторот. Подигнатиот под треба да биде

составен од панели/плочки кои на потребните места можат да се заменат со перфорирани плочи за дистрибуција на воздухот или прилагодени плочки за спроведување на кабли и сл. Со ваков дизајн се изолираат податочните кабли, струјните кабли и додатните цевоводи. Дополнително, со подигнатиот под се обезбедува лесна и ефикасна распределба на воздух и ладење кон хардверот. Иако е можно да се смести и прилагоди одредена количина хардвер и во поинаку дизајнирана сервер сала, високо препорачливо е системите да бидат инсталирани на подигнат под.

- Идеални височината на подигнатиот под треба да биде околу 60 cm, со обезбеден минимум од најмалку 46 cm. Отстапувањата од овие бројки треба да бидат базирани на дизајнот на системот за ладење и проценатa за потенцијално задушување под подигнатиот под како и потешкотии при реконфигурација (отстранување на неупотребени или дотраени кабли).
- Подните плочки треба да бидат со димензии 60 cm x 60 cm. Внатрешниот материјал од кој се изработени плочките може да биде од разни компримирани дрвени смеси или бетон, или од отворен метален дизајн. Целата плочка потребно е да е изработена или сместена во рамка од галванизиран или обоен челик. Алтернатива на ова се алуминиумски плочки.
- Горната површина на плочките треба да е од ламинат (high-pressure laminate). Површината на подот мора да обезбедува правилна дисипација на електростатички празнења. Подните плочки и структурната мрежа треба да се правилно заземјени. Потребно е да обезбеди минимум електричен отпор помеѓу подот и структурата под него.

- Чуварска служба

- Униформирана стражарска служба треба да патролира околу надворешниот периметар на податочниот центар, да го надгледува влезот со цел откривање на сомнителни активности и да ги прегледаат сите субјекти кои се упатуваат кон сервер салата.
- Сите припадници на чуварската служба треба да поминат ‘позадинска проверка’ потребна за утврдување на квалификациите и адекватноста за одреденото работно место.

- Надгледување

- Сите влезно/излезни точки и осетливи подрачја потребно е да се мониторираат со видео камери; надворешните камери треба да бидат изработени специфично за дневно-ноќна употреба; сите камери треба да бидат во заштитни кутии за да се спречи отворање и злоупотреба на опремата.
- Потребно е да се разгледа можноста за замена на старата аналогна опрема со понова дигитална опрема за мониторинг; дигиталните системи нудат подобрен визуелен квалитет, поврзување со стандардни компјутерски мрежи за пренос на податоци, ја олеснуваат централизацијата на мониторингот и се компатибилни со поновите комерцијални апликации кои се интегрираат со остатокот од информационите системи во организацијата.

- Надзор на климатско/временски услови

- Потребна е инсталација на детектори на чад за рано откривање на пожари.
- Потребна е инсталација на сензори за температура за надгледување на прегревање/преладување на сервер салата. Препорачливо е температурата да се одржува на константно ниво, најдобро во опсегот од 20 до 23 степени. Дополнително, потребно е да се инсталира сензор на секој шкаф со полици за опрема (rack) или на неколку локации во премините помеѓу шкафовите.
- Потребна е инсталација на сензори за влажност поради тоа што е можно празнење на статички електрицитет при ниски нивоа на влажност што потенцијално може да ја оштети опремата; при високи нивоа на влажност пак, можна е зголемена кондензација што исто така претставува опасност по опремата; потребно е влажноста во сервер салата да се одржува на константно ниво, препорачливо во опсегот од 45% до 55% релативна влажност.
- Кај уредите за климатизација мора да биде овозможена релативно голема точност, за температура +/-1º C и за влажност +/- 3% релативна влажност или помалку.
- Прецизните системи за ладење во сервер салата треба да имаат повисок размер на разменета топлина (sensible heat ratio - SHR) од уредите за просториите во кои работат луѓе. Идеално е сервер салата да има размер на разменета топлина 1:1, односно да обезбедува 100% ладење. Прецизните системи за ладење имаат помеѓу 85% и 100% ладење, додека повеќето нормални системи за ладење на простории имаат многу понизок процент.
- Системот за климатизација треба да се ре-конфигурира после секое додавање на хардвер кој претставува значителен извор на топлина.

- Филтрирање на воздухот

- Во случај да се утврди дека околината на сервер салата е во област со зголемено загадување на воздухот, потребна е инсталација на систем за филтрација на воздухот за отстранување на прашина, пестициди или индустриски нуспродукти бидејќи истите можат да ја оштетат електронската опрема па дури и да им пречат на одредени осетливи детектори на чад.
- Системот за ладење треба да биде дистрибуиран на таков начин што овозможува независен мониторинг и контрола на температурата на различните делови на систем салата.
- Потребно е да се земе предвид дека употребата на тавански системи за проток/ладење на воздухот може да предизвикаат турбуленции кои настануваат од интеракцијата на ладниот воздух со топлиот воздух кој природно се крева нагоре; алтернатива се механизми за ладење низ процепи од подигнатиот под, кои исфрлаат воздух нагоре низ перфорираните плочки на подот.
- Уредите за прецизно ладење треба да обезбедат соодветна промена на воздухот во климатизираниот простор. Додека на обичните работни простории им требаат само две промени на воздух на час, сервер салата со висока густина на

генератори на топлина може да има потреба и до 30 промени на воздухот на час. Затоа е важно избраните системи за прецизно ладење да можат да постигнат соодветен проток на воздух (повеќе од 0.24 m^3/s), за разлика од нормалните системи за климатизација (околу 0.17 m^3/s). Ако волуменот на проточниот воздух е несоодветен, дојдовниот разладен воздух ќе се загрева пред да стигне во областа која треба да ја разлади и со самото тоа ќе биде помалку ефективен во намалувањето на температурата во сервер салата.

- Против-пожарна заштита

- Потребна е инсталација на автоматски системи за заштита од пожар. Препорачлива е употреба на хемиски агенси и противпожарни апарати со што помало штетно дејство врз луѓето и ефективност против различни класи на пожари (Класа А/обични запаливи материи, Класа В/запаливи течности, Класа С/запаливи гасови, Класа Е/електрична опрема, Класа D/запаливи метали и Класа F/масти и масла).
- Рачни против-пожарни апарати потребно е да бидат сместени во просториите со опрема.
- Потребно е ѕидовите во просторијата со опрема да бидат премачкани со огноотпорна боја
- Системот за заштита од пожар треба да биде интегриран со системот за проток/ладење на водухот. За време на пожар, протокот на воздух од овие системи може да ја влоши ситуацијата со разнесување на пламенот.
- Потребно е да се избегнува сместување на непотребни и запаливи предмети во сервер салата. Дозволено е чување на минимум залихи на материјали потребни за функционирањето на сервер салата. Пакети, обвивки и друга амбалажа треба да се отстрани од сервер салата веднаш после распакувањето на опремата.
- Потребно е да се врши периодичен преглед на деловите на клима-уредите кои се загреваат интерно. Ако не се употребуваат подолг период, на истите се нафаќаат слоеви прашина кои можат да се запалат при вклучување на грејачот или загревање на деловите.
- Потребно е сервер салата периодично да се проверува за новонастанати пукнатини или други отвори. Ова може непотребно да ја изложи сервер салата на надворешни влијанија и сосем е неприфатливо алармните системи во сервер салата да се активираат поради надворешни услови.
- За помош и намалување на штетите при пожар потребно е организацијата да развие детални планови и да обезбеди соодветни обуки за персоналот задолжен за операции при пожар и други непогоди.

- Заштита од поплава

- Таваните, прозорците, вратите и ѕидовите мораат да бидат обезбедени/запечатени против пропуштање на вода од врнежи или поплави.
- Потребно е, каде што е можно, пренасочување на цевките со вода за истите да не поминуваат низ систем салата, а уште помалку над или под опремата

- Хигиенски средства (крпи, мопови) треба да бидат на дофат во случај на потреба на отстранување на помали количества вода.

- Сигурност на персоналот

- Потребно е во систем салата соодветно да бидат лоцирани мануелни контроли за различните системи за поддршка. Во идеален случај, контролите за против-пожарна заштита, заштита од протекување/поплава, климатизација, напојување и контроли за исклучување на аларми и независна телефонска линија, треба да бидат групирани покрај соодветните излези. Сите контроли треба да бидат видно означени со приложени кратки и јасни упатства за работа.

- Обезбедување на влезно/излезни точки

- Потребно е да постојат што помал број на влезни и излезни точки. Идеална ситуација е сите посетители да поминуваат низ единствена влезна точка. Овој влез е потребно да биде обезбеден со чуварска служба. Дупли врати за поединечен влез се често употребувана превентива за спречување на влез на неавторизирани лица кои можат да се прикрадат позади авторизирани лица ('piggy-backing').
- Излезите за итни ситуации треба да се отвораат само од внатре. Истите треба да се обезбедени со аларм и да се мониторирани.

- Автентикација

- Потребна е имплементација на јаки методи за автентикација на лицата. Препорачливо е користење на комбинација на механизми за автентикација (на пр.: употреба на картичка за пристап во комбинација со таен PIN код).
- Посебно јака заштита се обезбедува со употреба на биометриски методи. Со овие методи автентикација може да се прави со помош на геометрија на дланка, отпечаток од прст, скенирање на очниот ирис, скенирање на ретината и препознавање на глас. Автентикација со отпечаток од прст е често употребуван метод бидејќи оваа технологија е точна и згодна за употреба.
- Потребно е да се чуваат дневници со записи за влез/излез на сите лица (вклучително и посетители) кои физички пристапуваат кон податочниот центар.

- Резервни (редундантни) корисни средства

- Системите за напојување, греење, вентилација и ладење треба да имаат редундантни и backup системи. Струјата во зградата може да доаѓа од струјни линии од различни мрежи. Ако регуларниот довод на струја е прекинат, дизел генератори можат да бидат инсталирани за автоматско обезбедување помошен извор на струја.

- Каблирање

- Каблите за струја и мрежните кабли треба да бидат организирани/средени и да поминуваат или низ подигнат под или низ висечки тавански rack-ови.

- Мрежните кабли треба да бидат заштитени за превенција од интерференција (crosstalk).

- Означување на опремата

- Каблите, rack-овите со сервери и портовите треба да бидат јасно обележани со видливи етикети со цел на заштита од несакани грешки при инсталација и одржување на опремата.

- Сигурносни политики

- Според овие препораки потребно е да се воспостави формална сигурносна политика и истата да им се пренесе на сите вработени кои имаат пристап до сервер салата. Во зависност од конкретната имплементација на сервер салата, оваа политика би требало да ги пропише формално сите или одредени секции наведени во овој документ. На пример, според препораката за автентикација препорачливо е имплементација на јаки методи за автентикација на лицата и користење на комбинација на механизми за автентикација; соодветно, ако се избере, на пример биометриски тип на автентикација политиката официјално би пропишала користење само на таков тип на автентикација и забрана на автентикација со било која друга метода како превентивна контрола за оневозможување на заобиколување на сигурноста на влез во системите.

- Документација

- Потребно е да се документира локацијата и целта на опремата и каблите. Понатаму, потребно е да се документираат процедури за контактирање на испорачателот на секој од типовите на опрема, и истите да бидат лесно достапни. Потребно е да се донесат формални политики во врска со одржувањето на тековната документација.

- Справување со инциденти

- Потребно е да се развијат формални планови и вработените да се запознаат со истите. Плановите за справување со инциденти треба да ги покријат инцидентите чија причина е човечки фактор (провала), човечка грешка, опасности од околината (на пр.: пожар, поплава, висока температура, влажност), природни катастрофи (на пр.: земјотрес, невреме), и загуба на структурите за поддршка (на пр.: оштетување на зградата или загуба на електрична енергија).
- Плановите мора да вклучуваат упатства кои укажуваат ***кога*** е потребно да се контактира полицијата, противпожарната служба и кога треба да се алармира останатиот персонал во организацијата (на пр.: алармирање на персоналот за надоаѓачка опасност по човечка безбедност).
- Потребно е да се воспостават процедури за прибирање на докази, чување на докази и анализа на докази со цел утврдување на причината за инцидентот и/или подигање на судска постапка. Приложената предлог-процедура за управување со сигурносни инциденти (види прилог IM.01) ги дефинира постапките за справување со инцидент каде е опфатен и овој дел.

За успешно спроведување на наведените физички контроли, истите мора да бидат проширени и надвор од информациското опкружување и да вклучуваат ранливи точки низ целата организација до ниво на граници/заеднички точки со други организации. Ова може да вклучува оддалечени локации, изнајмени или заеднички простории. Дополнително, може да биде потребно осигурување дека слични контроли постојат и кај обезбедувачите на услуги (service providers) од кои организацијата користи производи и/или услуги, доколку истите се потенцијално ранливи и ризични за организацијата.

III. Процедура за управување со сигурносни инциденти

1. ЦЕЛ

Процедурата за управување со сигурносни инциденти има за цел да ги дефинира процесите, постапките и одговорностите за управување со сигурносните инциденти во информациониот систем на организацијата и известување кон раководството за постојните ризици.

Целта на овој документ е дефинирање и воспоставување на процес за брз и ефективен одговор на сигурносните настани, нивна ескалација, закрепнување од сигурносни настани и известување за сигурносните настани.

Со соодветна постапка на проценка на ризиците, нивно управување и планирање на одговорот на инцидентите се зголемува и способноста на организацијата успешно и брзо да одговори на инцидентите, да ги ограничи и да ги исправи настанатите штетни ефекти, како и да ги намали штетните последици на инцидентите во иднина.

Претпоставка за успешно планирање на одговорот на инцидентите е добро познавање на опкружувањето на информацискиот систем, познавање и следење на потенцијални закани, од една страна, и познавање на ранливите точки на системот од друга страна.

2. ОБЛАСТ НА ПРИМЕНА

Овој документ е применлив во активностите на Секторот за ИТ во организацијата и во секојдневните активности на корисниците на ИС во организацијата.

Оваа процедура ги опфаќа различните типови на настани и слабости, кои би можеле да влијаат врз сигурноста на информациските системи и/или податоци во организацијата.

3. РЕФЕРЕНТНИ ДОКУМЕНТИ

- Политика за сигурност на информациските системи,
- Политика за сигурност на лозинки,
- Политика за користење на Интернет
- Процедура за управување со back-up
- План за обука на корисниците/администраторите во согласност со сигурносната политика и процедурите
- Процедура за следење на настани во системот
- Процедура за бришење на податоци од медиумите
- Процедура за контрола на екстерен пристап кон ИС на организацијата
- Методологија за управување со ризици во ИТ/ИС на организацијата

4. ДЕФИНИЦИИ, ОЗНАКИ И КРАТЕНКИ

- **Инцидент** – непланиран и непосакуван настан чија последица е повредување (или непосредна закана за повредување) на важечките прописи, политиката за сигурност на информацискиот систем, останатите интерни акти на организацијата поврзани со информациската сигурност како и нарушување на темелните начела на информацискиот систем, прифатените практики во врска со информациската сигурност како и функционалностите на информацискиот систем.
- **Malware** – е софтвер дизајниран за инфилтрација или оштетување на информациски системи без знаење и согласност на сопственикот/корисникот. Ова е општ термин кој означува многу варијации/форми на интрузивен софтвер или софтвер/програмски код кој ја намалува продуктивноста поради неможноста за контрола на истиот. Организацијата може да дефинира листа на програми/типови програми кои ќе бидат означени како malware и чија злоупотреба ќе значи сигурносен инцидент.
- **IDS (Intrusion Detection System)** – Систем за детекција на упад во ИС, софтвер/хардвер кој детектира и забележува недозволени и неправилни активности или аномалии во мрежниот сообраќај.
- **Социјален инженеринг** - (анг. Social engineering) манипулација на корисниците со лажни тврдења и застрашување за придобивање на истите со цел на заобиколување на сигурносната заштита или откривање на доверливи податоци.

5. ОПИС

Во околината на ИС на организацијата се случуваат настани кои можат да ја нарушат сигурноста на системот. Овие настани се појавуваат во различни облици, а некои од инцидентите се појавуваат почесто од останатите. Со попишување на овие инциденти и подготовка на одговори на тие инциденти им се овозможува на вработените брзо и ефективно да реагираат на сигурносните закани.

Лицето одговорно за сигурност на информацискиот систем (ОСИС) во организацијата заедно со одговорните системски администратори треба да ги дефинира карактеристиките на честите сигурносни инциденти и постапките на одговор на овие инциденти. Потенцијалните сигурносни инциденти се дефинираат во согласност со проценатa на заканите по информацискиот систем во организацијата. Сигурносните закани и одговорот на сигурносните закани се дефинираат во посебен документ - **Сигурносни настани во ИС**, кој е приложен во оваа процедура. ОСИС заедно со одговорните системски администратори секои 6 месеци треба да го ревидира и ажурира документот - Сигурносни настани во ИС и по потреба да вклучуваат нови типови на закани по информацискиот систем во организацијата [1].

[1] За идентификација на нови типови на закани и нови потенцијални сигурносни инциденти корисно е, освен стандардните извори на информации за сигурноста на ИС (стручна

Примери на сигурносни инциденти се:

- загуба на услуга, опрема или уред
- неправилности во работата на уредите или системите,
- преоптоварување на уредите/системите,
- неусогласеност со интерните политиките и процедури и со соодветните важечки закони
- повреда на одредбите за физичка сигурност,
- неконтролирани промени во системот,
- повреда на правилата за пристап кон ИТ/ИС ресурси,
- кршење на доверливоста и интегритетот на податоците,
- злоупотреба на информациските системи

5.1 Основни упатства

Корисници

- Сите корисници на информациските системи треба да бидат запознаени со сигурносните мерки преземени за заштита на системите и информациите и како вработените да придонесат за зајакната сигурност на информациите.

Работни станици

- Сите работни станици/персонални компјутери е потребно да имаат инсталиран анти-вирусен/анти–malware софтвер
- Анти-вирус/анти–malware софтверот треба да биде конфигуриран така што при откривање на закана за системот да јавува соодветна порака, разбирлива за корисникот.
- Надградбите на програмот и дефинициите на вируси треба да бидат автоматски конфигурирани на одреден период и преземани од примарен сервер.
- Анти-вирус програмите треба да бидат конфигурирани така што корисникот да не може да ги стопира или деактивира истите, ниту да ги промени конфигурациите за заштита.
- Анти-вирус програмите треба да го скенираат и појдовниот и дојдовниот сообраќај на компјутерот.
- Целосно скенирање на компјутер може да биде изведено доколку Секторот за ИТ заклучи дека има потреба за тоа.

Апликациски сервери

- Сите сервери потребно е да имаат инсталиран анти-вирусен/анти–malware софтвер
- Надградбите на програмот и дефинициите на вируси треба да бидат

литература и слично) да се користат и попознати јавно достапни извори на информации како на пример «The National Vulnerability Database» на Институтот за стандарди и технологија на САД [URL: http://nvd.nist.gov/nvd.cfm]

автоматски конфигурирани на одреден период и преземани од примарен сервер.

- Примарниот сервер автоматски треба да ги спушта потребните документи од Интернет на дневна основа
- Потребно е скенирањето во реално време да е активно на серверите, а целосното скенирање може да биде распоредено по потреба во зависност од зафатеноста на серверите.

Email Сервери

- На сите електронски пораки кои имаат во прилог извршна програма (најчесто .exe, .vbs, .js, .bat attachment), прилогот треба да им се отстрани преку конфигурација на анти-спам модулот.
- На корисниците треба да им се забрани пристап до надворешни e-mail сервери со pop3 или imap пристап

5.2 Превентивни методи за спречување на сигурносни инциденти

5.2.1 Обезбедување на сигурноста на системите и податоците

Во организацијата постојат подготвени сигурносни политики и процедури, и работни процедури за обезбедување на сигурноста на информацискиот систем. Сигурносните политики и процедури во голема мерка помагаат во спречување на сигурносни инциденти и отстранување на закани по информацискиот систем. Под политики и процедури ги подразбираме следниве:

- Политика на сигурност на информацискиот систем,
- Правилник за одредување на надлежности и одговорности,
- Политика за сигурност на лозинки,
- Политика за користење на Интернет
- Процедура за управување со backup
- Процедура за следење на настани во системот
- Процедура за бришење на податоци од медиумите
- Процедура за контрола на екстерен пристап кон ИС во организацијата
- Имплементација на напредни технологии и добри пракси на управување со информацискиот систем на подрачјето на
    - физичка сигурност,
    - сигурност при комуникации,
    - логичка сигурност и контрола на пристап,
    - отстранување на сигурносни пропусти во програмскиот код на апликативниот и системскиот софтвер со закрпи и надградби (после процена на ризикот),
    - редовно ажурирање на антивирусна/анти-malware заштита,
    - други подрачја на информациска сигурност,
- План за обука на корисниците во согласност со сигурносната политика и процедурите
- Методологија за управување со ризици во информациското опкружување во организацијата

5.2.2 Тестирање на информацискатa сигурност во организацијата

Организацијата континуирано настојува да ја подобри сигурноста на своите клучни информациски системи и податоци. Дел од континуираниот процес на унапредување на сигурноста се редовните прегледи на подрачјата на информациска сигурност. ОСИС составува план на прегледи на секои 6 месеци. Планот на прегледи е составен така што зема предвид повеќе аспекти на информацискатa сигурност, а истовремено вклучува и прегледи во врска со нови типови на закани и нови потенцијални сигурносни инциденти.

Тестирањето на сигурноста од страна на ОСИС мора да биде документирано и за истото да се води архива.

5.3 Идентификација на сигурносни инциденти

5.3.1 Надзор на информациски систем и преглед на ревизорски записи (логови)

Администраторите на клучните системи редовно вршат надзор над системите за кои се одговорни, преглед на нивните параметри, преглед на податоците за дефинираните кориснички налози и преглед на дневникот на записи (логови) на системите.

ОСИС заедно со одговорните системски администратори ги дефинира типовите на автоматските логови на клучните информациски системи во организацијата. Потребно е да се дефинираат типови на настани кои ќе бидат следени во секој автоматски дневник, периодот на чување на записите од дневниците, фреквенцијата на преглед на дневниците и одговорно лице (позиција) за надзор на дневниците. Ревизорските траги ќе бидат дефинирани во посебен документ - Важни логови, кој е приложен во оваа процедура. ОСИС заедно со одговорните системски администратори ќе го ревидира и ажурира документот „Важни логови“ на секои 6 месеци.

Прегледите на дефинираните записи од дневниците се евидентираат во документот „Преглед на логови“, кој се наоѓа во прилог на оваа процедура.

Типични симптоми на сигурносен инцидент, на кои **администраторите на системот треба да обрнат посебно внимание** вклучуваат:

- системски аларми од IDS апликации / Анализатори на логови и необични записи во дневниците на firewall-овите, gateway-ите и останатите елементи на мрежата
- необични ставки во дневниците (на пример Windows корисник добива највисока системска привилегија – Administrator, без јасна причина или надвор од вообичаената процедура)
- недостаток на податоци во дневниците (на пример 30 минути од одреден период без било каков запис)
- неуспешни обиди за најава на системите
- необјасниви нови кориснички налози

- необјасниви нови датотеки и/или датотеки са необични имиња
- необјасниви промени на големината на датотеката и/или системските датуми, особено во извршните датотеки
- необјасниви обиди за записи во системските датотеки или промени на системски датотеки
- необјасниви промени или бришење податоци
- ускратување на услуга (анг. Denial of service)
- необјасниви падови на системот
- необјасниви забавувања на системот
- необични периоди на користење на системот (надвор од работно време)
- трагови на невообичаено користење на услуги (на пример, користење на апликативен модул од страна на корисник кој работи во друг сектор).

5.3.2 Пријавување на потенцијални сигурносни инциденти од страна на корисниците на информациските системи

Сите корисници, соработници по договор и надворешни соработници се одговорни за пријавување на потенцијални сигурносни инциденти. Службата за поддршка на крајните корисници на ИС (понатаму: Хелпдеск) служи како централно контактно место за пријава на потенцијалните сигурносни инциденти од страна на корисниците. Пријавувањето се врши на еден од следните начини:

- со повикување на телефонски броеви според пописот
- со испраќање на порака по електронска пошта на адреса според пописот

Пријава добиена по еден од дефинираните канали се прифаќа на обработка од Хелпдеск службата која е обучена да го прибележи инцидентот, да даде прво ниво на поддршка и во случај на потреба пријавата на инцидентот брзо да ја проследи кон администраторите на системот одговорни за истрага и решавање на инциденти во најкраток можен рок и со минимални трошоци.

Секоја пријава прифатена од страна на Хелпдеск службата мора да биде евидентирана и да ги опфаќа податоците за иницијаторот на барањето за помош, како и податоци за самото барање. Начелно, секое барање кон Хелпдеск службата се означува со одреден степен на итност и на решавање на проблемот:

- К = Критичен - проблеми кои потполно ја оневозможуваат употребата на системот
- В = Висок - проблеми кои ги оневозможуваат клучните системски функции без кои корисникот не може да ја води својата основна работа
- С = Среден - проблеми за чие решение може да се најде заобиколен пат
- Н = Низок - проблеми кои треба да бидат решени но за кои има заобиколен пат до решението и истото може да се користи на неодредено време.

Пријавите на потенцијални сигурносни инциденти секогаш се означуваат со степен на итност повисок од С.

За разлика од останатите кориснички барање кои доаѓаат до Хелпдеск службата, пријавите на сигурносни инциденти, во зависност од проценатa на Хелпдеск

службата, можат **веднаш да бидат проследени кон одговорниот администратор** а дополнително да се заведат во системот на службата за Хелпдеск.

Корисниците на системите брзо ги препознаваат и ги пријавуваат сигурносните инциденти кои потенцијално водат до загуба на услуга/сервис, опрема или уред. Освен овие очигледни сигурносни инциденти, корисниците мора да обрнат внимание и на останатите знаци на потенцијален сигурносен инцидент, како на пример:

- необични пораки од системите на своите монитори
- необјасниво забавување на системот
- воочени грешки во записите
- необични пораки во електронската пошта
- необични телефонски повици со прашања за доверливи информации (на пример лозинки) од страна на непознати лица – обиди за социјален инженеринг.

ОСИС периодично треба да организира активности на обука на крајните корисници во врска со различните аспекти на информациската сигурност, во кои ќе бидат вклучени и ажурни информации за честите сигурносни инциденти.

5.3.3 Истрага и решавање на сигурносни инциденти

Надлежните администратори на системот одговорни за истрага и решавање на инцидентите добиваат информација за потенцијален инцидент или од крајните корисници, преку Хелпдеск службата, или по пат на своите редовни активности за надзор над системите и преглед на дневниците.

5.3.3.1 Идентификација на инцидент

Одговорите на честите типови на сигурносни инциденти се дефинирани во посебен документ „Сигурносни настани“, кој е приложен кон овој документ.

Сигурносните инциденти кои не можат да се сместат во предефинираните категории мора да се анализираат прецизно за да се утврдат нивните причини. Тоа е основа за понатамошно управување со инцидентите.

5.3.3.2 Ограничување на инцидентите

По идентификацијата на инцидентот, следен приоритет е ограничување на неговите штетни последици. Прво, потребно е да се утврди што ќе се направи со загрозените информации и системи. Загрозените информации можат, меѓу другото, да бидат:

- Задржани во системот
- Копирани на екстерен електронски медиум
- Отстранети од системот

Слично, загрозениот систем може, меѓу останатото, да биде:

- Пуштен во продукциска околина под надзор

- Пуштен во продукциска околина, но со променети клучни параметри на системот (на пример лозинките на системските администратори)
- Неговите функционалности да бидат префрлени на друг систем
- Пуштен во продукциска околина, но исклучен од одредени мрежни сегменти
- Стопиран

5.3.3.3 Отстранување на инцидент

По ограничувањето на потенцијалната штета, администраторите треба да ги анализираат причините и сериозноста на инцидентот. Врз основа на оваа анализа, можат да се спроведат подобрувања на сигурносните параметри на информацискиот систем и трајно да се отстранат причините за инцидентот.

5.3.3.4 Закрепнување по инцидент

Фазата на закрепнување вклучува повторно воспоставување на компромитираните делови на информацискиот систем, како и проценка на состојбата и надзор врз деловните процеси. Кај релативно едноставните инциденти (на пример: неуспешен обид за упад во системот) доволно е администраторите да се уверат дека инцидентот немал штетно влијание врз информацискиот систем. Кај релативно комплексните инциденти (на пример: зараза со malware), закрепнувањето во некои случаи вклучува реставрација на системот од back-up медиуми и други комплексни операции.

Одредено време по завршувањето на фазата на закрепнување од инцидент, потребен е зголемен надзор над системот.

5.3.3.5 Осигурување на докази за инцидент

Доказите за инцидент се прибираат со цел да овозможат:

- Интерна анализа на проблемот,
- Форензични докази во врска со потенцијално кршење на договори или регулативни барања, или во случај на судска постапка,
- Преговори околу надомест на штета од страна на испорачателите на услуги или опрема.

Во случај по инцидентот да следи правна акција против одредено лице или организација, потребно е доказите да се приберат, сочуваат и претстават во согласност со прописите за приложување на докази.

Одговорниот администратор мора да ги зачува записите од дневниците, екранските прикази, резултатите на истрагата и другите доказни материјали, кои се собрани при истражувањето на причините за инцидентот. Онаму каде што е можно, доказите за инцидентот треба да се печатат или копираат на екстерни електронски медиуми. Одговорниот администратор рачно го запишува датумот и става свој потпис на доказите за инцидентот. Доказите мораат да се чуваат на

сигурно место (на пример во сеф) и да се забележат сите пристапи на вработените кон истите[2].

5.3.3.6 Известување за инцидент

По затворањето на инцидентот, одговорниот администратор е должен да напише извештај за инцидентот на стандарден образец - Извештај за инцидент.

Извештајот вклучува:

- Основни податоци за инцидентот: датум на пријава, име и презиме на вработениот кој го пријавил инцидентот, име и презиме на одговорниот вработен кој го презел решавањето на инцидентот и негови контакт податоци
- Податоците за компонентите на системот кај кои дошло до инцидент и нивната физичка локација
- Опис на инцидентот
- Опис на преземените мерки за ограничување на инцидентот,
- Опис на преземените мерки за закрепнување од инцидентот,
- Опис на доказите во врска со инцидентот и постапката на нивно чување.

5.3.3.7 Учење од сигурносни инциденти

Секои 6 месеци ОСИС ги анализира извештаите за инциденти и врз основ на анализата ги усогласува препораките за забрзано препознавање или спречување на појавата на инциденти од соодветен тип.

6. ОДГОВОРНОСТИ И ОВЛАСТУВАЊА

Корисниците на информацискиот систем се одговорни за пријавување на потенцијални сигурносни инциденати кон Хелпдеск службата. Сите вработени, соработници по договор и надворешни соработници треба да бидат запознаени со содржината на овој документот и да ги користат овде дефинираните постапки за известување во врска со сигурносни инциденти.

Лицето одговорно за сигурност на ИС е одговорно за следните работи: 1) дефинирање на процедура за управување со инциденти и нејзино ревидирање; 2) дефинирање на карактеристиките на честите сигурносни инциденти и постапки за одговор на инциденти; 3) дефинирање на превентивни методи за спречување на сигурносни инциденти; 4) дефинирање на постапки за преглед на записите (логовите)

Одговорните администратори на системите вршат редовен надзор над системите за кои се одговорни, преглед на нивните параметри, преглед на податоците за дефинираните кориснички налози и преглед на дневникот на записи (логови) на системите. Одговорни се за истрага и разрешување на инциденти.

[2] Одговорниот администратор во тие случаи бара и соработка од првната служба која е одговорна за деталите во постапките на управување со судски докази

Хелпдеск служба е одговорна за прием на пријави за потенцијални инциденти од страна на крајните корисници на информациските системи и проследување на пријавите кон одговорните администратори на системот.

Комитетот/одборот за информациска сигурност (IT Security Committee) е должен да ги ревидира извештаите за сигурносни инциденти со степен повисок од С на секои 6 месеци и за тоа да го извести раководството.

Ако начинот на задавање на задачите дефинирани во овој документ не е експлицитно дефиниран, тогаш се подразбира еден од следните начини на задавање задачи:

- во пишана форма
- преку електронска пошта

За контролата дали се постапува според овој документ овластен е _____ (ОСИС)

7. ПРЕГЛЕД НА ЗАПИСИ И ПРИЛОЗИ

Број	Ознака на образецот (број на прилог)	Назив на записот	Чување		
			Место	Начин	Време
1.		Важни логови	Архива на Секторот за информатика	Регистер	3 год
2.		Сигурносни настани	Архива на Секторот за информатика	Регистер	3 год
3.		Извештај за инцидент	Архива на Секторот за информатика	Регистер	3 год

Образец за листа на стандардни сигурносни настани во ИС

Овој документ претставува основна листа на потенцијалните сигурносни инциденти. Лицето одговорно за сигурност на ИС во организацијата и администраторите треба да ја дополнат листата со настани кои се релевантни во конкретната средина

Група на инцидент	Сигурносен настан	Одговорно лице за управување со инцидентот	Ограничување на инцидентот	Закрепнување по инцидентот
Интерни настани				
Инцидент - корисници	Неовластено користење на туѓ кориснички налог (на пример налог со администраторски права) на апликациите (..., ..., ...)	Одговорен администратор на системи (...)	Промена на лозинката на корисничкиот налог. Ревизија на користењето на останатите кориснички налози со големи права и промена на лозинките на сите кориснички налози со администраторски или супер-администраторски права	Интерна истрага на настанатата штета и враќање на податоците /системите во изворна/почетна состојба.
Инцидент - корисници	Неовластено користење на туѓ кориснички налог (на пример налог со администраторски права) на ниво на оперативен систем, на компјутери во домен, надвор од домен или на мрежни уреди	Одговорен администратор на системи (...)	Промена на лозинката на корисничкиот налог. Ревизија на користењето на останатите кориснички налози со големи права и промена на лозинките на сите кориснички налози со администраторски или супер-администраторски права	Интерна истрага на настанатата штета и враќање на податоците /системите во изворна/почетна состојба.
Инцидент - уреди	Испад на клучна хардверска компонента на информацискиот систем	Одговорен администратор на системи /мрежен администратор	Во согласност со дефинираната постапка од disaster recovery планот	Во согласност со дефинираната постапка од disaster recovery планот
Инцидент - корисници	Неовластена комуникација со доверливи податоци надвор од организацијата (на пример со преносни медиуми) - Откривање на	Лице одговорно за сигурност на ИС	Забрана на понатамошна комуникација	Интерна истрага за настанатата штета и акционен план заедно со одговорните за односи со јавност и правна служба

	деловна тајна			
Инцидент - корисници	Значителна грешка која ја загрозува сигурноста на процесирањето на критична апликација или значително ја успорува работата	Одговорен администратор на системи (...)	Во согласност со дефинираната постапка од disaster recovery планот	Во согласност со дефинираната постапка од disaster recovery планот
Инцидент - уреди	Ненамерно уништување на хардверски уред	Одговорен администратор на системи /мрежен администратор	Замена на хардверскиот уред	Интерна истрага за настанатата штета вклучувајќи ја и штетата настаната поради потенцијалната загуба на податоци
Екстерни настани				
Инцидент - уреди	Испад на електрична мрежа	Одговорен администратор на системи /мрежен администратор	Во согласност со дефинираната постапка од disaster recovery планот	Во согласност со дефинираната постапка од disaster recovery планот
Инцидент - уреди	Испад на јавна телекомуникациска мрежа	Одговорен мрежан администратор	Во согласност со дефинираната постапка од disaster recovery планот	Во согласност со дефинираната постапка од disaster recovery планот
Инцидент - уреди	Кражба на хардверски уреди (работни станици, мрежни уреди)	Одговорен администратор на системи /мрежен администратор	Замена на хардверскиот/мрежниот уред	Интерна истрага на настанатата штета вклучувајќи ја и штетата поради потенцијална повреда на сигурноста на податоците
Инцидент - услуги	Ускратување на услуга (напад со Denial of Service)	Одговорен мрежен администратор /администратор на системи	Повторно воспоставување на сервисот (рестарт, враќање од backup, ...)	Интерна истрага Евентуално зголемување на бројот на расположливи линкови
Инцидент - физичка сигурност	Природна катастрофа	Лице одговорно за сигурност на ИС	Во согласност со дефинираната постапка од disaster recovery планот	Во согласност со дефинираната постапка од disaster recovery планот
Инцидент - корисници	Социјален инжинеринг - манипулација на корисниците со лажни тврдења и застрашување со цел заобиколување на сигурносните контроли и/или откривање на податоци	Лице одговорно за сигурност на ИС	Предупредување на корисниците да не откриваат податоци кои се деловна тајна или потенцијално претставуваат опасност по деловна тајна ако се откријат	Интерна истрага на настанатата штета вклучувајќи ја и штетата поради потенцијална повреда на сигурноста на податоците Повторување на обуки за подигање на свесноста за сигурност на информации

Инцидент - надворешни корисници на системите	Phishing - Обид за наведување на корисниците (преку лажни e-mail пораки кои изгледаат веродостојно) кон откривање на доверливи лични податоци со нивно несакано пренасочување кон лажирани web страни	Лице одговорно за сигурност на ИС	Предупредување на корисниците кои се потенцијални жртви на phishing	Интерна истрага на податоците собрани за време на евентуални phising напади (IP адреси и други идентификациони податоци) Истрага на настанатата штета вклучувајќи ја и штетата настаната поради повреда на сигурноста на податоците
Инцидент - корисници	Hoax - пораки преку електронска пошта со невистинита содржина, испратени со цел на застрашување, измама или дезинформирање на примачот	Лице одговорно за сигурност на ИС	Предупредување на корисниците да не шират hoax пораки	Интерна истрага за изворот на hoax пораките (ако инцидентот е доволно сериозен за тоа да е потребно)
Инцидент - корисници	Spam, junk mail или несакана комерцијална пошта со рекламна содржина	Лице одговорно за сигурност на ИС	Предупредување кон корисниците да не преземаат никакви акции кои евентуално се предложени во пораката	Подобрување на постојните spam филтри Намалување на бројот на јавно достапни објавени e-mail адреси на вработените во организацијата
Инцидент - софтвер	Вируси, макровируси, црви, тројанци	Одговорен администратор на системи /мрежен администратор	Извршување на прелед на медиумите со антивирус/анти-malware програми	Интерна истрага на настанатата штета вклучувајќи ја и штетата поради потенцијална повреда на сигурноста и интегритетот на податоците
Инцидент - логичка сигурност	Хакерски/кракерски пробивања на сигурноста и пенетрација	Одговорен мрежен администратор /администратор на системи	Запирање на сите акции/сервиси кои напаѓачот ги извршува со кориснички налози со администраторски права Запирање на сите акции/сервиси кои напаѓачот ги извршува со кориснички налози со обични кориснички права	Интерна истрага на податоците собрани за време на нападот (ИП адреси и други идентификациони податоци) Истрага на настанатата штета вклучувајќи ја и штетата настаната поради повреда на сигурноста на податоците

Образец: Извештај за инцидент

1. Идентификациски податоци за инцидентот:

Ознака на инцидентот:	Идентификациски број на инцидентот
Датум на пријава на инцидентот:	Датум кога инцидентот прв пат е забележан
Симптоми на инцидентот (означи ги сите релевантни симптоми):	☐ Необични пораки на екранот ☐ Необјасниво забавување на системот ☐ Воочени грешки во записите ☐ Необични пораки во електронската пошта ☐ Необични телефонски повици со прашања за доверливи информации(на пример лозинки) од страна на непознати лица – обид за социјален инженеринг ☐ Системски аларми од ИДС алатите ☐ Необични записи во дневниците на firewall-от, gateway-от и другите елемента на мрежата ☐ Необични записи во системските дневници ☐ Недостаток (gap) на податоци во дневниците ☐ Неуспешни обиди за најава на системите/апликациите ☐ Необјасниви нови кориснички налози ☐ Необјасниви нови датотеки и/или датотеки со необични имиња ☐ Необјасниви промени на величините на датотеките и/или системските датуми, посебно во извршните датотеки ☐ Необјасниви обиди за запис во системските датотеки или промена на системските датотеки ☐ Необјасниви промени или бришење на податоците ☐ Прекин на услуга (Denial of service) ☐ Необјаснив пад на системот ☐ Необјасниво забавување на работата на системот ☐ Необични периоди на користење на системот ☐ Траги на невообичаено користење на апликации/сервиси/услуги ☐ Друго: Опис на други релевантни симптоми
Додатни информации:	Додатен опис на потенцијалниот сигурносен инцидент (ако е потребно)
Пријавувач на инцидент/барање:	Име и презиме на корисникот (вработен, соработник по договор и надворешен корисник)
Сектор / дирекција:	Сектор на вработениот кој го пријавува инцидентот
Физичка локација на инцидентот:	Работна единица, локација

2. Идентификација на инцидентот:

Одговорен администратор:	Име и презиме и функција на одговорниот администратор кој го презел решавањето на инцидентот
Датум на почетокот на решавањето на инцидентот:	Датум на преземање на решавањето на инцидентот од страна на одговорниот вработен во Службата за ИТ

Погодени систем(и):	Листа на директно и индиректно погодени системи
Извор на инцидентот	☐ Надворешен извор ☐ Внатрешан извор
Тип на инцидент:	☐ Надворешно провалување во системот ☐ Прекин на услуга (Denial of service) ☐ Неправилно користење на информациските ресурси (неовластено користење на туѓ кориснички налог, неовластен пристап кон податоци,...) од страна на легитимни корисници ☐ Вирус / malware програм ☐ Социјален инженеринг ☐ Hoax пошта ☐ Spam пошта ☐ Phishing ☐ Испад на хардверска компонента ☐ Испад на електрична мрежа ☐ Испад на јавна комуникациска мрежа ☐ Ненамерно уништување на хардверски уред ☐ Неовластено откривање на доверливи податоци надвор од организацијата - Откривање на деловна тајна ☐ Друго: Опис на други типови на инцидент
Опис на инцидентот:	На пример: - име на вирусот, црвот, тројанецот - тип на hoax - опис на провалата во системот

3. Ограничување и закрепнување после инцидентот

Чекори за ограничување на инцидентот:	Опис на преземените чекори за ограничување на инцидентот
Чекори за закрепнување од инцидентот:	Опис на преземените чекори за закрепнување од инцидентот

4. Анализа и отстранување на инцидентот

Последици на инцидентот:	Опис на последиците од инцидента врз податоците, клучните компоненти на ИС, угледот на организацијата ...
Целокупна процена на влијанието на инцидентот:	☐ Мал инцидент – инцидентот нема значајно влијание на податоците и системите во организацијата ☐ Среден инцидент – инцидент до одредена мера влијае на податоците и системите во организацијата ☐ Голем инцидент – инцидент значајно влијае на податоците и системите во организацијата
Чекори за отстранување на инцидентаот:	Опис на чекорите преземени за отстранување на инцидентот
Следни планирани чекори:	☐ Пријава на инцидентот на надлежните органи ☐ Отпочнување на правна акција ☐ Интерна дисциплинска акција ☐ Друго: Опис на други релевантни чекори
Останати информации:	

IV. Процедура за управување со промени во информациските системи

1. ЦЕЛ

Со оваа процедура прецизно се дефинира постапката за предлагање на промени, разгледување на предлози и донесување на одлуки за реализација на промените со цел подигање на квалитетот на работата на вработените и системите кои се користат во организацијата.

2. ОБЛАСТ НА ПРИМЕНА

Оваа процедура ја применуваат сите вработени кои предлагаат промени во рамките на информациските системи во организацијата.

3. РЕФЕРЕНТНИ ДОКУМЕНТИ

- *Место за идни референци*

4. ДЕФИНИЦИИ, ОЗНАКИ И СКРАТЕНИЦИ

a. HW - хардвер
b. SW - софтвер
c. User acceptance test – тест со кој се потврдува дека промените се во согласност со корисничкото барање
d. IT Steering Committee - орган во организацијата кој се занимава со управување на ИТ проекти
e. Test case – еден од случаите во тестна околина

5. ОПИС

Оваа процедура ги опфаќа сите промени кои се однесуваат на работата на информацискиот систем во рамки на организацијата.

Барање за промена може да поднесе секој вработен во организацијата.

Барањето се поднесува во пишана/електронска форма, на образецот **Baranje_za_promena.doc**, кој се наоѓа на мрежна локација предвидена за чување на процедури и обрасци (\\fileserver\documentfolder\...).

Потребно е подносителот на барањето да го пополни документот „**Барање за промена**“ и тоа на следниот начин:

- Подносителот во заглавието, во предвидените полиња на документот ги внесува датумот, својата функција, име и презиме.

- Бројот на документот се формира на следниот начин: на префиксот eGov- му се додава датум во формат ггммдд, а потоа и шифрата/интерниот број на работникот и реден број на неговото барањето за тој ден.

На пример: ако Петар Петровски со шифра *xyz* на ден 19.05.2011 година поднесе 2 (две) барања, неговите документи ќе ги добијат следните броеви:

eGov-110519-xyz-1 и eGov-110519-xyz-2

- Подносителот на барањето е должен да специфицира дали бараната промена треба да се спроведе во тестна или продукциска околина, од кој тип е барањето (HW, SW, апликации, податоци), кој е објектот на кој треба да се изврши промената, поради која причина се бара промената, кои се очекуваните ефекти и колку е итно спроведувањето на промената.
- Подносителот на барањето е должен да:
    - Го отпечати документот "**Барање за промена**", да го потпише и да го упати на разгледување на _____ (пр. Директорот на својот сектор) и на одговорната личност за ИТ прашања, кои ја сочинуваат основата на **Тимот за анализа на барањата за промена**, или
    - Електронски да го потпише и да го испрати по електронска пошта на разгледување на _____ (пр. Директорот на својот сектор) и на одговорната личност за ИТ прашања, кои ја сочинуваат основата на **Тимот за анализа на барањата за промена**.

Во зависност од околината во која е потребно да се спроведе промената, областа и објектот на кои се однесува предлог-промената, споменатиот Тим може да биде проширен со цел што поквалитетна анализа на предлогот.

Водачот на Тимот за анализа на барањата за промена (пр. Директорот на соодветниот сектор) организира состанок на Тимот заради разгледување на оправданоста и можноста за реализација на предложените промени.

Тимот за анализа на барањата за промена врши процена на предложените промени и ги дополнува со информации за потребните материјални (HW и SW) и кадровски ресурси, планирани трошоци, можни последици и со планираниот начин за проверка на успешноста на предложената промена. Врз основа на ова Тимот донесува **Одлука за предложената промена**. Во зависност од проценката на времето потребно за реализација на промената Тимот предложува термини за реализација на промените.

Предложените промени се спроведуваат во согласност со постојните процедури и упатства во организацијата и документи поврзани со нив.

Членовите на Тимот со своите потписи во Одлуката за предложената промена ја потврдуваат својата согласност или образложена несогласност, заедно со анализата на предлогот за промена.

Водачот на Тимот за анализа на барањата за промена го запознава Директорот на Секторот за информатика со барањето за промена и со донесената одлука на Тимот.

Директорот на Секторот за информатика, во пишана форма, на документот **Одлука за предложената промена**, дава своја согласност на донесената одлука и одредува лице одговорно за реализација.

Доколку Тимот за анализа на барањата за промена заклучи дека промената бара големо ангажирање на ресурси, било да се тие од страна на информациските технологии или од страна на одговорните оперативни функции, **IT Steering Committee** може да го дефинира проектот така што ќе одреди: спонзор на проектот, цел, потребни ресурси, временски тек на имплементацијата, задолженија и овластувања на секој од членовите на тимот за реализација. Во овој случај следењето на проектот го превзема IT Steering Committee.

Во зависност од потребните ресурси и трошоци на проектот раководството на организацијата може да утврди износ потребен за реализација, над кој, за реализација на промената неопходно е одобрување од страна на IT Steering Committee.

Во случај на одобрување на барањето, лицето одговорно за реализација на промената на извршителот/реализаторот на барањето му го проследува документот **Барање за промена** заедно со придружните документи. Придружни документи се:

- **Прашалник за промена**

- **Извештај за извршена промена**

Намената на првиот документ (Прашалник за промена) е размена на дополнителни информации иницирана од страна на извршителот со цел попрецизно појаснување на барањата и очекувањата кои ги изнел подносителот на барањето.

За секое Барање за промена се користи еден документ 'Прашалник за промена'. Потписник на прашалникот е одговорното лице од страна на организацијата/секторот Извршител. По спроведувањето на промените, Извршителот треба да спроведе соодветни тестови пред да ги дистрибуира направените промени до подносителот на барањето.,

Во Извештајот за извршената промена Извршителот ќе наведе дали промената е успешно реализирана, а потоа ќе внесе опис на направените промени и спецификација на потрошените ресурси. Потпишаниот Извештај потоа се упатува кон подносителот на барањето.

Подносителот на барањето потоа ќе спроведе соодветен user acceptance test. Потребно е овој тест да се спроведе по реализираната промена од страна на Извршителот и пред имплементација на промената во продукциската околина.

Тестното сценарио и резултатите од тестирањето подносителот на барањето ги внесува во Извештајот за промена во табелата наменета за тоа. Доколку финалниот резултат на тестирањето е позитивен, подносителот на барањето со потпис ја потврдува валидноста на реализираните промени и со тоа се создаваат предуслови за имплементација на промените. Следен чекор е ажурирање на соодветната придружна документација доколку истата не е изменета при реализацијата на промената.

Доколку user acceptance test-от не даде задоволителни резултати, подносителот на барањето му враќа негативен извештај на Извршителот заедно со придружна документација (неуспешни test case-ови).

6. ОДГОВОРНОСТ И ОВЛАСТУВАЊА

Кон овој документ мора да се придржуваат сите учесници процесот на промени во информациските системи на организацијата.

Ако начинот на задавање на задачите дефинирани во овој документ не е експлицитно дефиниран, тогаш се подразбира еден од следните начини на задавање задачи:

- во пишана форма
- преку електронска пошта

За контролата дали се постапува според овој документ овластен е _____ (Директорот на секторот за информатика)

7. ПРЕГЛЕД НА ЗАПИСИ И ПРИЛОЗИ

Во врска со оваа процедура, како резултат на извршување на наведените активности, се водат записите дадени во Табела 1.

Табела 1

Број	**Ознака на образецот (број на прилог)**	**Назив на записот**	**Чување**		
			Место	**Начин**	**Време**
1.	*eGov-CM-1*	Барање за промена	Архива на Секторот за информатика	Регистер / Back-up медиум	5 год
2.	eGov-CM-2	Одлука за предложената промена	Архива на Секторот за информатика	Регистер / Back-up медиум	5 год
3.	eGov-CM-3	Извештај за промена	Архива на Секторот за	Регистер / Back-up медиум	5 год

			информатика		
4.	eGov-CM-4	Прашалник за промена	Архива на Секторот за информатика	Регистер / Back-up медиум	5 год

ОБРАЗЕЦ – БАРАЊЕ ЗА ПРОМЕНА

БРОЈ НА БАРАЊЕ	НАЗИВ НА ДОКУМЕНТ	ДАТУМ НА БАРАЊЕ
	БАРАЊЕ ЗА ПРОМЕНА	

ПОДНОСИТЕЛ НА БАРАЊЕТО	ФУНКЦИЈА	ИМЕ И ПРЕЗИМЕ	ПОТПИС

1. ПРОМЕНАТА ДА СЕ ИЗВРШИ ВО:

☐ Тестна околина

☐ Продукциска околина

☐ Друго _____

2. ОБЛАСТ

☐ Hardware

☐ Системски software (ОС, А/В...)

☐ Апликација

☐ Податоци

☐ Мрежа

☐ ...

3. ОБЈЕКТ ВРЗ КОЈ СЕ ИЗВРШУВА ПРОМЕНАТА

4. КРАТОК ОПИС НА БАРАНАТА ПРОМЕНА И ОЧЕКУВАНИ ЕФЕКТИ

5. ПРИОРИТЕТ И ПРИЧИНИ

БРОЈ НА ОДЛУКА	БРОЈ НА БАРАЊЕ	НАЗИВ НА ДОКУМЕНТОТ	ДАТУМ НА ОДЛУКА
		ОДЛУКА ЗА ПРЕДЛОЖЕНА ПРОМЕНА	

	ФУНКЦИЈА	ИМЕ И ПРЕЗИМЕ	ПОТПИС
ТИМ ЗА АНАЛИЗА НА ПРЕДЛОГ-ПРОМЕНАТА			
ОДЛУКА	☐ **ПРИФАТЕНО** ☐ **ОДБИЕНО**		

СОГЛАСНОСТ НА ДИРЕКТОРОТ НА СЕКТОРОТ ЗА ИТ	
СОГЛАСНОСТ НА IT STEERING COMMITTEE	

МИСЛЕЊЕ НА ТИМОТ ЗА АНАЛИЗА НА ПРЕДЛОГ- ПРОМЕНАТА

1. ПОТРЕБНИ МАТЕРИЈАЛНИ РЕСУРСИ (HW/SW) (и предлог на начин за обезбедување)

2. ПОТРЕБНИ КАДРОВСКИ РЕСУРСИ (и предлог на начин за обезбедување)

3. ПЛАНИРАНИ (ОЧЕКУВАНИ) ТРОШОЦИ (и предлог на начин за обезбедување)

   HW:

   SW:

   ЧОВЕЧКИ РЕСУРСИ:

4. ПЛАНИРАНО ВРЕМЕТРАЕЊЕ НА РАБОТАТА

   ВРЕМЕТРАЕЊЕ НА РАБОТАТА:

   ИТНОСТ:

   РОК ЗА ЗАВРШУВАЊЕ:

5. ПРОДУКТИ / ПРОЕКТИ ВРЗ КОИ ВЛИЈАЕ ПРОМЕНАТА

ДИРЕКТНО:

ИНДИРЕКТНО:

6. МОЖНИ ПОСЛЕДИЦИ (согледани, очекувани)

ВО СЛУЧАЈ ДА НЕ СЕ СПРОВЕДЕ ПРЕДЛОЖАТА ПРОМЕНА:

ВО СЛУЧАЈ НА ОДЛОЖУВАЊЕ НА ПРОМЕНАТА:

ВО СЛУЧАЈ НА ГРЕШКА/ПРОБЛЕМ ЗА ВРЕМЕ НА ВОВЕДУВАЊЕТО/ПО ВОВЕДУВАЊЕТО НА ПРОМЕНАТА:

7. ПЛАНИРАН НАЧИН НА ПРОВЕРКА НА УСПЕШНОСТА НА ПРОМЕНАТА

ОПИС НА ПОСТАПКАТА (НАЧИНОТ) ЗА ПРОВЕРКА:

ВРШИТЕЛ НА ПРОВЕРКАТА:

ПРЕДЛОГ ЗА КОНТРОЛЕН ОБРАЗЕЦ:

8. ПЛАНИРАНИ ПОСТАПКИ ЗА ОПОРАВУВАЊЕ (Во случај на неуспешност на промената)

9. КОМЕНТАР

БРОЈ НА ИЗВЕШТАЈ	БРОЈ НА БАРАЊЕ	НАЗИВ НА ДОКУМЕНТ	ДАТУМ НА ИЗВЕШТАЈОТ
		ИЗВЕШТАЈ ЗА ПРОМЕНА	

ОДГОВОРЕН ЗА РЕАЛИЗАЦИЈА	ФУНКЦИЈА	ИМЕ И ПРЕЗИМЕ	ПОТПИС
ИЗМЕНА	☐ **РЕАЛИЗИРАНА** ☐ **НЕ Е РЕАЛИЗИРАНА**		

ОБРАЗЛОЖЕНИЕ НА ИЗВРШИТЕЛОТ

10. ОПИС НА ПРОМЕНАТА

11. ПОТРОШЕНИ РЕСУРСИ

    HW:

    SW:

    ЧОВЕЧКИ РЕСУРСИ:

    ДАТУМ И ВРЕМЕ НА ЗАВРШУВАЊЕТО:

    ВКУПНО ПОТРОШЕНО ВРЕМЕ:

12. КОМЕНТАР

ТЕСТИРАЊЕ НА ПРОМЕНАТА

ПОДНОСИТЕЛ НА БАРАЊЕТО	ФУНКЦИЈА	ИМЕ И ПРЕЗИМЕ	ПОТПИС
ТЕСТИРАЊЕ	☐ **УСПЕШНО** ☐ **НЕУСПЕШНО**		

13. ОПИС НА ТЕСТОТ

Модул	Опис на функционалноста	Резултат на тестот	Коментар

14. КОМЕНТАР

БРОЈ НА ПРАШАЛНИК	БРОЈ НА БАРАЊЕ	НАЗИВ НА ДОКУМЕНТ	ДАТУМ НА ПРАШАЛНИК
		ПРАШАЛНИК ЗА ПРОМЕНА	

ОДГОВОРЕН ЗА РЕАЛИЗАЦИЈА	ФУНКЦИЈА	ИМЕ И ПРЕЗИМЕ	ПОТПИС

ПРАШАЊА И ОДГОВОРИ

Прашање:	Датум на прашање:
Одговор:	Датум на одговор:

Прашање:	Датум на прашање:
Одговор:	Датум на одговор:

Прашање:	Датум на прашање:
Одговор:	Датум на одговор:

V. Политика за употреба и сигурност на лозинки

1. ЦЕЛ

Целта на овој документ е формално да дефинира политика во организацијата која се однесува на употребата и сигурноста на лозинките. Потребно е сите вработени да бидат запознаени со истата и да се придржуваат до упатствата изнесени подолу.

2. ОБЛАСТ НА ПРИМЕНА

Политиката за употреба и сигурност на лозинките (понатаму Политиката) се однесува на сите корисници на информацискиот систем на организацијата (вработените на неопределено време; вработените на определено време; вработените со скратено работно време; лица ангажирани преку Агенции за привремени вработувања; лица кои работат на извршување на проект; други лица како стажанти, надворешни лица, странски консултанти, бизнис партнери и испорачатели на услуги).

3. РЕФЕРЕНТНИ ДОКУМЕНТИ

- Политика за сигурност на ИС во организацијата

4. ДЕФИНИЦИИ, ОЗНАКИ И КРАТЕНКИ

Кориснички налог – множество на права и привилегии над оперативен или информациски систем. По правило корисничкиот налог се врзува за физичко лице. Корисникот се идентификува во системот со помош на своето корисничко име и лозинка.
ИТ ресурси – ги вклучуваат сите сервери, мрежи, компјутери, документи, како и сите форми на гласовна, видео и електронска комуникација, и комуникациски уреди во организацијата.

5. ОПИС

Со оваа политика за употреба и сигурност на лозинки се дефинираат:

- типовите на лозинки
- правила на генерирање
- век на траење
- кои лозинки треба да се чуваат во писмена форма
- место на чување
- постапка на чување и пристап до лозинките во случај на оправдана потреба
- постапка на замена на лозинки на кои им истекува рокот на траење
- начин на евиденција на секој пристап кон лозинките

5.1 Одредби за сите типови лозинки

За пристап кон компјутерите, апликациите и електронските сервиси во организацијата, заради спречување на неовластен пристап се отвораат кориснички налози со придружни лозинки.

Лозинките кои се користат за пристап кон информациските системи се делат на администраторски и кориснички, при што се применуваат различни правила за нивно доделување, век на траење, промена и чување.

Зависно од **можностите, потребите и проценетата ризичност на поединечни информациски системи/платформи**, потребно е лозинките да се креираат така што да ги задоволат следните минимални барања:

- да имаат определена најмала должина (на пр.: 8 знаци)
- да исполнуваат услови за комплексност на лозинката;

На пр.: лозинката мора да исполнува најмалку три од следните четири правила и тоа да содржи:

- големи букви (на пример: A, B, C)
- мали букви (на пример: a, b, c)
- броеви (на пример: 0, 1, 2)
- специјални знаци (#, &, !, %, |, ?, -, *)
- ист знак не смее да се појавува повеќе од ___ (два) пати

- да исполнува услови за несодржење на поими кои лесно се поврзуваат со корисникот (името на корисникот или зборови / изрази кои често се користат или кои лесно асоцираат на корисникот, имиња на членови од семејството, имиња на домашни миленици, родендени ...)

- да се имплементира механизам за одреден број погрешни обиди за внес (дозволени се до ___ (3) последователни погрешни обиди за внес на лозинката во рок од ___ (30) минута, после што корисничкиот налог се заклучува; заклучувањето на корисничките налози е со траење од 30 минути, додека администраторските налози се заклучуваат на неопределено време, односно додека не ги ослободи член на администраторската група)

- да се имплементира контрола при промена на лозинката да не можат повторно да се користат одреден број последно користени лозинки (10)

Лозинките имаат ограничен век на траење, односно рок до кога најдоцна мораат да се променат. Векот на траење се одредува за секој клучен ресурс во организацијата посебно, и може да биде најмалку 1 ден, а најмногу 60 денови. Секој клучен ИТ/ИС ресурс во организацијата мора да биде конфигуриран така што ќе форсира промена на лозинката по истекот на нејзиното траење.

Лозинките се тајни. Секој корисник е должен да ја чува тајноста на својата лозинка и не смее да ја открива на други корисници. Секој корисник е одговорен за злоупотреба на корисничкиот налог, било поради невнимателно чување или намерно откривање на лозинката на други корисници.

5.2 Администраторски лозинки

Во администраторски лозинки спаѓаат лозинките на сите администраторски налози на серверите односно мрежните уреди наведени во **Референтната листа на клучните информациски ресурси** на организацијата.

Администраторските лозинки се тајни, и само овластени администратори на поединечните клучни ресурси имаат право да ги знаат. Секој од клучните компјутерски ресурси во организацијата има доделен еден или повеќе администратори кои се наведени во **Референтната листа на компјутерски администратори** во организацијата.

Администраторските лозинки имаат ограничен век на траење, односно рок до кога најдоцна мора да бидат променети. Векот на траење се одредува посебно за секој клучен информациски ресурс на организацијата, и може да биде најмалку 1 ден а најмногу 45 дена. Освен задолжителната промена на лозинката по истекувањето на рокот на траење, секој администратор, односно корисник на лозинка е должен да иницира постапка за промена на лозинката секој пат кога постои сомневање дека неовластено лице ја дознало лозинката.

Администраторските лозинки се чуваат во писмена форма во пликови во посебен сигурносен сеф кој гласи на организацијата и се користи исклучително за таа намена. Раководителот на Секторот за информатика и Лицето одговорно за сигурност на информациските системи (ОСИС) се овластени личности кои имаат пристап кон сефот. Раководителот на Секторот за информатика и Лицето одговорно за сигурност на информациските системи можат да им дадат право на пристап кон лозинките и на други лица. По правило, ова можат да бидат лицата од Референтната листа на компјутерски администратори во организацијата.

На сигурносниот сеф, овластените лица можат да му пристапуваат поради редовни причини (одлагање на нови или изменети лозинки во сефот, поради истекување на рокот на траење) или поради вонредни причини (преземање на лозинки во оправдано потребна ситуација, а личноста која е овластена за нивна употреба не е достапна, и во ситуација на вонредна промена на лозинката за која постои сомневање дека е достапна на неовластени лица).

Секој пристап кон сигурносниот сеф мора да го направат две лица, од кои барем едно мора да биде овластен администратор или заменик на администраторот за соодветниот клучен информациски ресурс на организацијата чија лозинка е

потребна. Ова лице се потпишува во листот за евиденцијата во колоната “Лице 1”. Другото лице посведочува на извршениот пристап со потпис во листот за евиденцијата во колоната “Лице 2”.

За секој пристап направен поради вонредни причини, лицето кое пристапило кон сигурносниот сеф должно е да го извести Лицето одговорно за сигурност на информациските системи (ОСИС) истиот ден, односно најдоцна следниот работен ден, ако пристапот е направен надвор од работното време на организацијата. Во истиот рок е потребно да се направи и вонредна промена на лозинката.

Лозинката за секој администраторски налог кој се однесува на ресурс од Референтната листа на клучни информациски ресурси на организацијата се чува во посебен плик на кој треба да биде напишан називот на серверот (ресурсот, средството) и називот на администраторскиот налог.

Секој плик се користи за еднократно чување на лозинката. На лист хартија е потребно е да се запишат/испечатат називот на серверот, називот на администраторскиот налог и лозинката и истиот се сместува во пликот. Пликот треба да биде залепен, со печат на организацијата на местото на спојување и преку печатот треба да се залепи самолеплива лента со чие отстранување видно се оштетува втиснатиот жиг.

При секој друг пристап кон сигурносниот сеф, лицата кои пристапиле се должни да ги запишат своите податоци во листата за евиденција на пристапот која се наоѓа во самиот сигурносен сеф со пликовите за лозинки. Со еден пристап кон сигурносниот сеф можно е да се заменат повеќе пликови, а за секој плик се запишува датумот на пристап, називот на пликот (односно називот на серверот и администраторскиот налог), ознака дали пристапот е од редовен или вонреден тип и опис на промената.

Секој пристап кон сигурносниот сеф се забележува во листа за контрола на пристап. На барање на Лицето одговорно за сигурност на информациските системи (ОСИС), задолженото лице за надзор на пристапот кон сигурносните сефови е должно да ја предаде на увид.

Лицето одговорно за сигурност на информациските системи (ОСИС) има право и обврска на повремена проверка дали во сигурносниот сеф се наоѓаат пликовите за сите клучни информациски ресурси во организацијата, и дали евиденцијата на пристап уредно се пополнува и одговара на стварната содржина на сефот. Пристапот со цел проверка, ОСИС го извршува заедно со лице од Референтната листа на компјутерски администратори во организацијата.

Доколку ОСИС утврди неправилност во пристапот кон сигурносниот сеф, или отворени пликови, може да иницира итна вонредна замена на сите лозинки кои се чуваат во сигурносниот сеф, и за тоа да состави записник.

5.3 Кориснички лозинки

Кориснички лозинки се лозинки на корисничките налози наменети за контролиран пристап на крајните корисници кон апликациите и сервисите. Корисничките налози се конфигурирани така што да им овозможуваат на корисниците пристап кон апликациите, но не и пристап кон административните алатки.

Кориснички налог на корисникот, за поединечен информациски ресурс на организацијата, му отвора администраторот на тој ресурс, на барање на одговорното лице во организационата единица во која работи корисникот. Одговорното лице кон администраторот упатува барање по обична или електронска пошта. При отворањето на корисничкиот налог, администраторот поставува иницијална лозинка, и во писмен облик му го предава лично на корисникот неговото корисничко име и соодветната лозинка, го упатува како сам да ја промени својата лозинка и го информира за неговите одговорности.

Корисникот при првиот пристап кон системот е должен да ја промени иницијално добиената лозинка.

Корисничките лозинки не подлежат на обврска за чување во сигурносен сеф.

За корисничките лозинки важат сите правила за комплексност, траење и тајност наведени во делот за општи одредби.

Во случај кога работникот подолго време не го користи својот налог поради отсуство, промена на работите кои ги извршува или престанок на работниот однос во организацијата, администраторот привремено го блокира налогот, и тоа на барање на одговорното лице од организационата единица во која работи корисникот. Барањето на администраторот му се предава во писмена форма или преку електронска пошта.

Измени и дополнувања на оваа Политика врши ОСИС, кој е должен да ги запознае со последната верзија сите администратори од Референтната листа на компјутерски администратори во организацијата. Согласност за измени и дополнувања на оваа Политика дава Генералниот секретар или друго лице со соодветни овластувања со потпис на два пишани примероци, од кои еден се наоѓа кај ОСИС, а друг кај Раководителот на секторот за информатика.

6. ОДГОВОРНОСТ И ОВЛАСТУВАЊА

Кон овој документ мора да се придржуваат сите вработени во организацијата како и сите останати корисници кои пристапуваат кон ИС во организацијата.

- Секторот за ИТ е одговорен за:
    - администрација на правата за пристап на корисниците
    - редовен надзор на сигурноста на ИТ ресурсите
- Вработените се одговорни за:
    - Почитување на оваа процедура

Ако начинот на задавање на задачите дефинирани во овој документ не е експлицитно дефиниран, тогаш се подразбира еден од следните начини на задавање задачи:

- во пишана форма
- преку електронска пошта

За контролата дали се постапува според овој документ овластено е _____ (Лицето одговорно за сигурноста на информацискиот систем)

7. ПРЕГЛЕД НА ЗАПИСИ И ПРИЛОЗИ

Број	Ознака на образецот (број на	Назив на записот	Чување		
			Место	Начин	Време
1.		Референтна листа на клучни информациски ресурси во организацијата	Архива на Секторот за информатика	Регистер / Back-upмедиум	3 год
2.		Референтна листа на компјутерски администратори во организацијата	Архива на Секторот за информатика	Регистер / Back-upмедиум	3 год