



РЕПУБЛИКА МАКЕДОНИЈА  
МИНИСТЕРСТВО ЗА ИНФОРМАТИЧКО ОПШТЕСТВО И АДМИНИСТРАЦИЈА  
**08/2-4567/1**  
**29.11.2012 година**

**ПОЛИТИКА  
НА  
ИНФОРМАЦИСКА И КОМУНИКАЦИСКА ТЕХНОЛОГИЈА  
(ИКТ) ВО МИНИСТЕРСТВО ЗА ИНФОРМАТИЧКО  
ОПШТЕСТВО И АДМИНИСТРАЦИЈА**

Практиката покажува дека е невозможно однапред да се предвиди појавувањето на секоја различна ситуација, а ова предизвикува вработените да донесуваат различни одлуки во рамките на политиката на ИКТ. За таа цел, а воедно за да им се помогне на вработените да бидат доследни и ефикасни во одлуките, развиен е овој документ.

Овој документ обезбедува рамка за покривање на широк опсег на активности и воспоставување на принципи, со кои треба да се обезбеди ефективна работа во Министерството за информатичко општество и администрација (во понатамошниот текст Министерството).

ПОЛИТИКА НА ИНФОРМАЦИСКА И КОМУНИКАЦИСКА ТЕХНОЛОГИЈА (ИКТ) ВО МИНИСТЕРСТВО ЗА ИНФОРМАТИЧКО ОПШТЕСТВО И АДМИНИТРАЦИЈА		
Историја на ревизии		
Верзија	Датум	Опис на ревизијата
01	31.10.2011	иницијална
Подготовка		
Овој документ е подготвен од:		
Функција	Име и презиме	Потпис
Р.О.	м-р Игор Марковски	
Согласен		
Овој документ е проверен од:		
Функција	Име и презиме	Потпис
Државен секретар	м-р Јахи Јахија	
Одобравања		
Овој документ е одобрен од:		
Функција	Име и презиме	Потпис
министер	м-р Иво Ивановски	
Дистрибуција		
Функција	Име и презиме	
<a href="http://www.miow.gov.mk">http://www.miow.gov.mk</a>	До сите вработени во МИОА	

## Содржина

ЦЕЛ.....	4
Принципи .....	4
Дефиниции.....	4
ИКТ Полиса.....	5
Вовед.....	5
Одговорности.....	5
Персонал за поддршка на ИКТ – систем администратори .....	6
Користење на опремата .....	6
Полиса за обуки .....	7
Начела за добро користење користење на опремата .....	8
Лична употреба на опремата.....	8
Неприфатлива употреба на опремата .....	9
Персонални прашања.....	10
Одговорности на персоналот.....	11
Одговорности на надворешни корисници.....	11
Корисници-гости .....	11
Категории на пристап .....	12
Полиса за лозинки.....	12
Вовед.....	12
Полиса.....	13
Промена на лозинка.....	14
Системски лозинки - Барања за систем администратори.....	14
Поврзување сметачска опрема на мрежата .....	15
Огнен ѕид и ВПН (виртуелна приватна мрежа) .....	16
Полиса за електронска пошта.....	16
Употреба на Интернет.....	18
Лаптоп полиса.....	20
Телефони.....	20
Одржување и безбедност на веб-локација на Министерството.....	21
Ревизија на софтвер и хардвер.....	21
Преместување на опрема .....	21
Резервни копии и враќање на податоците.....	21
Сервери и ажурирање на безбедноста на локалните системи .....	22
Вирусна полиса и процедура .....	22
Физичка безбедност.....	23
Процедури за системско тестирање.....	23
Отстранување на стара опрема .....	24
Вовед.....	24
Полиса.....	24
Procedures - процедури.....	25
Техничка поддршка на корисници.....	26
Споделување на податоци.....	26
Конвенција за именување на документи .....	27
Чувствителни информации.....	28
Користење на фонтови .....	28

## ЦЕЛ

Целта на овој документ е да се одреди политиката на Министерството за информатичко општество и администрација (МИОА), во однос на дефинирање прифатлива и забранета употреба на информатичката и комуникациска технологија (ИКТ). Оваа политиката се однесува на потребата за заштита на Министерството во целина, на вработените, како и на другите органи на државната управа кои ги користат информациските системи на МИОА, и ќе послужи како појдовен основ за градење стабилни релации во понатамошната соработка на Министерството и неговите системи со други институции и системите кои тие ги користат.

Вработени во Министерството кои користат ИКТ системи и ИКТ ресурси на други институции, при користење на тие истите, се да ги почитуваат политиките на користење на ИКТ ресурсите на тие институции.

## Принципи

Принципи кои ја изразуваат основната цел на оваа полиса се:

- Министерството ќе обезбеди пристап до информациско комуникациски технолошки ресурси на соодветни лица во согласност со потребите и расположливите ресурси.
- Министерството очекува законско, етичко и одговорно користење на неговите ИКТ ресурси.
- Министерството ќе ги преземе сите мерки на претпазливост за да ја заштити безбедноста и приватноста на своите ИКТ кориснички сметки, и за таа цел ги информира корисниците дека нормалната употреба и одржување на системите вклучува и креирање на резервни копии, и периодичното надгледување на користењето на опремата/системите, во насока на нивна заштита.
- Министерството ги вреднува и почитува принципите на слобода на изразување, барајќи истите да бидат одговорно практикувани.

## Дефиниции на користени поими

За целите на оваа полиса, освен ако не е поинаку назначено, важат следните дефиниции:

Корисничка сметка	Било кој сметачки или комуникациски ресурс доделен на корисник од страна на Министерството и заштитен од генерална употреба преку безбедносен систем (т.е. лозинка).
-------------------	--

ИКТ (Информациско комуникациска технологија)	ИКТ вклучува технологии како пероснални и преносни сметачи, софтвер, приклучни уреди, телефонска опрема (вклучително мобилни телефони) и интернет врски чија намена е исполнување на информациско-процесиращки и комуникациски функции.
ИКТ ресурси на Министерството	Сите мрежи, хардвер, софтвер и комуникациски услуги и уреди кои се во сопственост, доделени или користени со дозвола од страна на Министерството.
Мрежа на министерство	Централна ИКТ мрежа и други мрежи обезбедени од страна на структури на Министерството, и опрема (т.е. лично поседувани сметачи) кои се поврзани во мрежата на Министерството, за целите на овој документ ќе бидат сметани како дел од мрежата на Министерството.
Корисник, Овластен корисник	'Корисник' и 'Овластен Корисник' – ги подразбира сите вработени, како во Министерството така и на проекти, корисници-гости, и надворешни корисници кои од страна на Министерството се овластени да пристапуваат кон неговите системи и/или мрежа.

## ИКТ Полиса

### Вовед

Целта на овој дел од документот е обезбедување на процедури и полиси, насоки и препораки за обезбедување на мрежата и електронските податоци во сопственост на Министерството за информатичко општество и администрација. Овој документ им е располагање на раководството и сите вработени во Министерството.

### Одговорности

Сопственикот на корисничка сметка од Министерството, или на сметачки систем поврзан со Министерството, одговорен е за активностите поврзани со корисничката сметка или сметачкиот систем.

Корисниците и овластените корисници, мора да ги преземат сите мерки за заштита на нивната опрема и, каде што тоа е случај, на деталите и лозинките

од нивните сметки.

## **Персонал за поддршка на ИКТ – систем администратори**

Персоналот за поддршка на ИКТ – систем администраторите, во однос на секој од системите на МИОА, ги определува министерот.

Функции на систем администраторите се, но не и ограничени на:

1. имплементација на ИКТ Полисите на Министерството.
2. стручна поддршка при набавки на опрема, и обезбедување опремата која се набавува да има гаранција со соодветен рок.
3. проценување на потреби за ИКТ опрема, и грижа за сите прашања во врска со ИКТ потребите на Министерството, особено за прашања поврзани со мислења и технички совети за ИКТ иницијативи во Министерството.
4. водење на ажурни списоци на опремата во Министерството.
5. одржување на опремата, каде спаѓаат и следните одговорности:
  - Хардвер дијагностицирање на едноставни грешки – проблеми со каблирање, со печатење, или не функционирање на мемориски уреди и носители.
  - Инсталација на софтвер - Анти-вирус и кориснички програми
  - Сервисирање и инсталација на сметачи и периферни уреди
  - Администрација на мрежа – споделување на ресурси и документи

## **Користење на опремата**

Ефикасното и исплатливото користење на ресурсите од Информациско комуникациската технологија (ИКТ) се базира на правилно користење и распоредување на соодветна и доволна ИКТ опрема и софтверска инфраструктура.

Ова вклучува:

### Хардвер:

- персонални сметачи
- сервери
- преносни сметачи
- печатачи
- скенери
- мултифункционална опрема
- мрежни рутери и прекинувачи
- уреди за континуирано електрично напојување (УПС)
- проектори

- мрежна опрема
- дигитални фотоапарати и камери
- ЦД/ДВД-и Ром
- клима уреди во сервер салите
- телефони
- опрема за складирање податоци - Storage

#### Софтвер:

- оперативни системи
- Апликативен софтвер
- Анти-вирусни програми
- Сопствено развиени системи

Персоналот за поддршка на ИКТ ресурсите е одговорен за безбедност на целата опрема и податоците на Министерството. За да се обезбеди соодветна и континуирана функционалност, треба да се спроведуваат следните безбедносни мерки:

- Серверите и мрежните уреди треба да бидат инсталирани во обезбедени и добро проветрени простории, и снабдени со доволно моќност за напојување преку правилно тестирани уреди за континуирано електрично напојување /УПС-и/.
- За да се избегне вирусна инфекција од внатре, пред употреба на надворешни носители на меморија (ЦД/ДВД, флеш дискови, итн.) истите задолжително претходно да се скенираат и да се провери безбедноста од нивното користење.
- соодветно чување на гаранција на сета сметачска опрема и софтвер во употреба.
- влез во Сервер салата му е дозволен само на персоналот за поддршка на ИКТ - систем администратори.
- сите податоци кои се однесуваат на Министерството, треба да бидат зачувани на соодветен медиум за резервни копии.
- редовни проверки на системите
- известувања за случени инциденти

#### **Полиса за обуки**

Информатичката технологија е област во постојан развој. Оттука, се инсистира на постојана обука на вработените за новите технологии со што ќе се елиминира можноста, Министерството да заостане со трендовите. За да се обезбеди доволна обученост на корисниците за оперирање со сметачките системи, но и за стручна поддршка кон стратешките цели на Министерството и другите институции:

- сите засегнати корисници ќе бидат обучени соодветно за секој нов софтвер или хардвер.

- персоналот за поддршка на ИКТ треба да биде конзистентно обучуван да дејствува како прво ниво на ИКТ поддршка во организацијата.
- министерството ќе обезбеди релевантни ИКТ материјали за учење на персоналот за поддршка на ИКТ.
- министерството ќе обезбеди релевантни едукативни материјали за учење на вработените, за користење на ИКТ системите.

### **Начела за добро користење на опремата**

Министерство за информатичко општество и администрација обезбедува електронски комуникациски системи и услуги за вработените во Министерството, вработените во други органи на државна управа и за граѓаните. Сепак, употребата на овие средства се состои од прифаќање на оваа полиса и е предмет на следниве ограничувања, кој се неопходни за доверливо функционирање на електронските комуникациски системи и услуги:

- вработените мора да ги почитуваат сите важечки закони.
- електронските средства треба да се користат според нивната намена.
- вработените мора да ги почитуваат правата, приватноста и сопственоста на другите.
- вработените мора да се придржуваат до правилата за доверливост со кои се регулира безбедната употреба на лозинки и сметки, чии детали не смеат да се споделуваат.
- лозинките не смее да бидат обзнанувани никому дури и ако станува збор за друг вработен во Министерството. Привремените лозинки дадени од страна на персоналот за поддршка на ИКТ мора да се променат веднаш по првото успешно најавување.

Вработените при привремено напуштање на работното место мора да го почитуваат принципот “чист екран“ и во случај на неактивност на сметачот во период подолг од 5 минути, истиот треба да биде подесен автоматски да се заклучи.

### **Лична употреба на опремата**

Опремата на Министерството за информатичко општество и администрација инцидентно може да се користат за лични цели, но под услов:

- целите да се од приватен карактер, а не за финансиска добивка и да не се во спротивност со било кои други полиси кои го засегаат персоналот;
- таквата употреба да не предизвикува забележливи или неизбежни трошоци за Министерството;



- таквата употреба да не влијае несоодветно врз официјалната работа на Министерството;
- таквата употреба да не вклучува било какви активности забранети во делот ИКТ полиси и процедури на прифатлива употреба;

### **Неприфатлива употреба на опремата**

ИКТ средствата на Министерството не смее да бидат давани на привремено користење на индивидуални корисници или организации надвор од Министерството, освен кога дозвола за таква услужна поддршка е доделена од страна на државниот секретар и тоа само за владини организации/институции.

Опремата на Министерството не може да се користи за следните активности:

- создавање, дистрибуција, складирање и прикажување на непристојни или порнографски материјали;
- создавање, дистрибуција, складирање и прикажување на непристојни слики од деца;
- создавање, дистрибуција, складирање и прикажување на литература на омраза;
- создавање, дистрибуција, складирање и прикажување на материјали кои промовираат тероризам;
- создавање, дистрибуција, складирање и прикажување на клеветнички материјали или материјали кои може да бидат навредливи за другите;
- симнување, складирање и дистрибуирање на авторски заштитени материјали, вклучувајќи софтвер и секакви форми на електронски податоци, без дозвола на носителот на авторското право или надвор од условите на лиценци кои се набавени од Министерството;
- сите активности кои не се во согласност со важечките закони во врска со заштитата на интелектуалната сопственост и податоци. Посебен акцент е ставен на симнување и копирање на музички и видео записи преку интернет со користење на peer-to-peer клиенти за споделување на документи. Во согласност со законите кои се однесуваат на правата од интелектуална сопственост, симнување и копирање на датотеки како што се, MP3, AVI, DivX и било какви други електронски формати на аудиовизуелни дела без дозвола на сопственикот на авторските права е противзаконски;
- намерно мешање или стекнување незаконски и неовластен пристап до кориснички сметки и податоци, вклучувајќи гледање, менување, уништување или оштетување на податоци кои припаѓаат на други корисници;
- употреба на корисничко име и лозинка кои припаѓаат на друг корисник;

- обиди за пробивање на лозинки или декодирање на енкриптирани податоци;
- секоја друга употреба која може да доведе во прашање угледот на Министерството или да го изложи на ризик од судски постапки;
- намерно или несовесно создавање, извршување, проследување или внесување на било какви вируси, црви, тројанци или софтверски кодови создадени за оштетување, самореплицирање или попречување на перформансите на мрежата на Министерството;
- намерни дејствија кои би можеле да ја намалат ефикасноста на антивирусот или на друг ИКТ безбедносен софтвер инсталиран од страна на овластен персонал на Министерството;
- обиди за навлегување во безбедносните мерки (хакирање), без разлика дали резултатот би имал или немал загрозување или губење на податоци;
- намерно скенирање на внатрешни или надворешни машини во обид за откривање или експлоатација на познати софтверски или мрежни слабости;
- ангажирање во комерцијални активности кои не се под покровителство на Министерството;
- користење на сметачки ресурси (процесор, време, простор на дискот, и пропустен опсег) на начин што ја нарушува работата или безбедноста на системите или создава проблеми за други корисници;
- поврзување било каков сметачки уред на мрежата на Министерството, само ако ги исполнува безбедносните стандарди утврдени од страна на персоналот за поддршка на ИКТ мрежата.

## **Персонални прашања**

Персоналот за поддршка на ИКТ ја одржува листата на лица кои ги користат ИКТ ресурсите на Министерството. Вработените, надворешните и гостинските корисници се предмет на условите за користење на ИКТ на Министерството, но имаат различни права и обврски.

За целите на оваа полиса

- Вработени во Министерството се оние лица кои се регистрирани во системите за Одделението за човечки ресурси.
- Вработени на проекти се лица кои работат за Министерството и се финансираат од буџет на проект.
- Корисници – гости, се луѓе со дозволен привремен пристап до јавните ИКТ ресурси на Министерството. За да им овозможи на корисниците вработените - гости строго ограничен пристап до јавните ИКТ ресурси на Министерството, се користат гостински кориснички сметки.
- Надворешен корисници / вклучувајќи волонтери, и др. се сите други

лица на кои им е дозволено пристап до ИКТ системите на Министерството.

## **Одговорности на вработени**

Сите вработени (вклучувајќи ги привремените корисници и персоналот на проекти) мора да се согласат на пишани правила и услови за користење на ИКТ кога се регистрираат за користење на ИКТ на Министерството.

Услугата за персоналот треба да обезбеди:

- обуката за подигање на свесност за безбедност на електронски информации да биде дел од програмата за обуки на вработените во Министерството.
- информациите за безбедноста на електронски информациите да ги има во прирачниците за сите вработени.
- корисничките сметки на времено вработените да бидат поставени да истекуваат на крајот на нивниот договорен период.

## **Одговорности на надворешни корисници**

Надворешните корисници мора во писмена форма да се запознаат и да се согласат на Условите и правилата пред/за да добијат корисничка сметка. Евиденција на овие согласности и се води од страна на Персоналот за поддршка на ИКТ мрежата.

Надворешните кориснички сметки се со ограничено траење (максимум 12 месеци), а доколку е потребно истите ќе се продолжуваат според условите наведени во овој документ.

## **Корисници-гости**

Кориснички сметки за гости може да се отворат/креираат, за да им се овозможи на посетителите строго ограничен пристап до јавните ИКТ ресурси на Министерството. Одобрение за отварањето на сметките дава Државниот секретар МИОА202Р1 Пишана евиденција на оваа ИКТ употреба се води од страна на одговорните за установата.

Пристап до корпоративните системи, заштитените електронски ресурси, услугите на електронска пошта на Министерството и сопствените/локалните капацитети за зачувување на документи, нема да им бидат дадени на користење на корисниците - гости.

## Категории на пристап

Пристапот до ИКТ е ограничен во зависност од типот на корисник. Вработени во Министерството или на проект и надворешни корисници може да ги користат:

- Стандардното софтверско портфолио
- Споделен склад на документи
- е-пошта, календар и јавни папки<sup>1\*\*</sup>
- Деловни системи на Министерството<sup>2 \*\*</sup>
- Интернет

Корисниците гости може да ги користат:

- Стандардното софтверско портфолио
- Интернет

## Полиса за лозинки

### Вовед

Информации зачувани на персонални и преносни сметачи, и на LAN (Local Area Network) се сопственост на Министерството. Министерството води еднозначна средина со најавување, при што корисникот може да добие пристап до сите мрежни ресурси користејќи едно корисничко име и лозинка, поткрепени со цврста полиса за лозинка.

Лозинките се примарен метод на автентификација пред користење ИКТ ресурси на Министерството и во моментот се основен метод за идентификување. Лозинките обезбедуваат само овластени лица да имаат пристап до определени сметачки системи и воспоставување на одговорност за сите промени направени на системските ресурси. Силните лозинки промовираат безбедна сметачка околина; лошо избрани лозинки ги загрозуваат информациите кои би требало да ги заштитат.

Ако корисничкиот профил е блокиран, сопственикот на истиот треба да испрати барање за да му се оспособи профилот до персоналот за поддршка на ИКТ – систем администраторите, со праќање на електронска порака на [it\\_helpdesk@mioa.gov.mk](mailto:it_helpdesk@mioa.gov.mk).

---

<sup>1</sup> Овие услуги нема да им бидат овозможени на сите надворешни корисници (на пример, претставници на надворешни организации со сопствени е-пошта сметки).

<sup>2</sup> Овие услуги нема да им бидат овозможени на сите надворешни корисници (на пример, претставници на надворешни организации со сопствени е-пошта сметки).

Доколку корисникот ја заборави својата лозинка, треба лично да се обрати до персоналот за поддршка на ИКТ мрежата и да побара нејзино ресетирање, со праќање на електронска порака на [it\\_helpdesk@mioa.gov.mk](mailto:it_helpdesk@mioa.gov.mk).

Корисниците мора да се воздржуваат од одговарање на електронски пораки во кои се бара од нив да го дадат своето корисничко име и лозинка поради одржување на системот, дури и ако се чини дека пораката е од Персоналот за поддршка на ИКТ мрежата. Таквите пораки се фиктивни и се обид за кражба на идентитетот на корисникот за нечесни цели.

### **Полиса за лозинките**

- лозинките треба да се чуваат во тајност и да не се споделуваат со колегите.
- корисничкото име или негови варијации не треба да бидат вградени во лозинка.
- лозинките не смее да бидат празни.
- Сметачски генерираните лозинки мора да се сменат по иницијалното успешно најавување.
- лозинките не треба да се базираат на лични податоци (на пример имињата на семејства, миленичиња, името на вашата улица, автомобилски регистарски броеви, броеви на телефон)
- лозинките не смее да му се откриваат на вашиот директен претпоставен.
- лозинките не смее да се соопштуваат по телефон, дури и ако примачот е член на Персоналот за поддршка ИКТ мрежата.
- лозинките што се користат во рамките на Министерството не смее да се користат за надворешни интернет сметки.
- лозинките што се користат во рамките на Министерството не се препорачува да се користат за надворешни сметки.
- лозинките мора да се разликуваат од претходните лозинки. Претходните лозинки не треба повторно да се употребуваат.
- новите лозинки не треба да бидат ни малку слични со претходните. Откако лозинката ќе се промени, новата лозинка мора да биде во функција најмалку 8 дена пред да му се дозволи на корисникот повторно да ја промени.

### **Добри практики**

Лозинките не треба да бидат вклучени во било кој автоматски процес на најавување, а особено ако станува збор за заеднички сметачи.

Лозинките не треба да биде испишувани, испраќани преку електронска пошта или соопштувани по нивно ресетирање.

Лозинките не треба да се внесуваат или зачувуваат во електронски документи.

### **Поставување на лозинка**

Лозинките за десктоп / клиент оперативни системи треба да ги исполнуваат следниве критериуми:

- Лозинките мора да бидат од барем осум карактери.
- Лозинките треба да бидат составувани од алфанумерички карактери (букви – a...z, A... Z, цифри - 0 ... 9), но треба да вклучуваат и специјални карактери (на пример: & % \$ и сл.). Лозинката треба да содржи најмалку една голема буква, една мала буква, една цифра и еден специјален карактер
- Лозинките треба да бидат силни (да не е лесно да бидат погодени или автоматски генерирани)

### **Промена на лозинка**

Лозинките мора да се менуваат при било која од следниве околности:

- Најмалку еднаш на секои шест месеци, а при апликации кои обработуваат лични податоци на секој три месеци..
- Веднаш, ако лозинка е искомпромитирана или ако се сомневате дека е компромитирана.
- По инструкција на персоналот за поддршка на ИКТ.

Забелешка: Не е препорачливо да се менува лозинката во петок попладне или непосредно пред заминување на одмор бидејќи праксата покажува дека веројатноста да биде заборавена е голема.

### **Системски лозинки - Барања за систем администратори**

Привилегираните и административните лозинки мора да бидат со строго силен состав и висока честота на промената. Привилегирани лозинки се лозинки за рутери, свичеви, хабови, огнени ѕидови, мрежни оперативни системи како и сите други ИТ системи / ресурси.

За секој ИКТ систем, барем двајца членови на ИКТ персоналот мора да имаат привилегии/пристап. За привилегирани и административни лозинки, се води евиденција кој администратор/лице за поддршка на ИКТ мрежата има пристап до кој систем. Сите лозинки треба да бидат документирани во книга на лозинки и секогаш да се чуваат во сеф. Само министер/државен секретар може да пристапува до сефот.

Лозинките за секој сервер систем мора да бидат единствени.

Определен број на заеднички локални административни лозинки може да се користат на машини за специфични локации.

Лозинките мора да бидат барем осум карактери, а по можност и подолги.

Лозинка за рутерите никогаш не смее да се користи не-криптирана низ мрежата за да се избегне 'прислушување'.

Лозинките мора да се повлекуваат по шест месеци употреба.

Откако лозинка ќе се промени, новата лозинка мора да биде на функција барем 8 дена пред на корисник да му се дозволи повторно да ја смени.

Услужни сметки не смее да се базираат на администраторски сметки/лозинки.

На сметките создадени за надворешни изведувачи треба да им се доделат рестриктивни права за извршување на своите функции, а сметките треба да се блокираат веднаш по завршувањето на назначената задача.

Администраторски /привилегирани лозинки не смее да бидат откриени на надворешни изведувачи.

Предефинираните лозинки кои доаѓаат со сметачки системи или услуги мора да се променат за време на инсталацијата или системот треба да се подеси така да го потсети администраторот да ја смени лозинката при следната најава.

Новопоставената лозинка мора да биде различна од претходно користените лозинки. При новопоставената лозинка, не смее повторно да се користат последните десет користени лозинки.

Критичните системи мора да вградат полиси за отклучување на сметки и да се постават така што да ги исклучуваат неактивните сесии по период на неактивност од триесет минути.

Системите мора да бидат конфигурирани да принудуваат промена на лозинки по однапред дефинирана фреквенција.

Привилегираните лозинки не треба да се комуницираат преку телефон факс или е-пошта.

Поврзување сметачска опрема на мрежата

Во Министерството, мрежна пристапна точка која е доделена на конфигуриран сметач/сметач, не смее да се користи од страна на друг сметач.

Сметачи, работни станици и преносни сметачи, ПДА и паметни телефони смеат да бидат поврзан на мрежата Министерството исклучиво од страна на персоналот за поддршка на ИКТ.

На корисниците кои сакаат директно да поврзат персонални сметачи на мрежата, истото им е дозволено само преку официјално назначени физички порти или безжични пристапни точки.

Се забранува поврзување лични преносни сметачи на мрежата на Министерството. Во исклучителни случаи, корисниците кои сакаат да ја поврзат нивната лична опрема на мрежата, истите мора да добијат одобрување од страна на министер/државниот секретар на Министерството. Во тие случаи важат следните принципи:

- нивниот оперативен систем и било кој инсталиран софтвер треба да биде целосно премостен.
- ажуриран антивирус и заштита од софтвер за шпионирање треба да се инсталира за да се обезбеди заштита од вируси, црви, штетни програми или уреди или било што друго чија цел е да се меша во, да ги прекинува или нарушува нормалните оперативни процедури на мрежата на Министерството.
- треба да се инсталира личен firewall за да се обезбеди заштита од неовластен упади.

Огнен ѕид и VPN (виртуелна приватна мрежа)

Огнените ѕидови (firewalls) се суштествени за било која мрежна инфраструктура. Огнениот ѕид е критичен елемент во заштитата на локални мрежи (LAN), VPN широки мрежи (WAN), или комбинација од истите, од неовластен упад, вируси, црви, и потенцијални напади за негација на услуга. Иако огнениот ѕид не е лек за сите овие потенцијални закани, тој е важен и клучен елемент во обезбедувањето на било која мрежа. Министерството користи Microsoft ISA за заштита на LAN и VPN врски. Целите системи имаат статички IP адреси и редовно се следат и ажурираат.

Полиса за електронска пошта

Министерството обезбедува електронски поштенски услуги ("електронска пошта") на сите вработени. Системот се одржува од страна на персоналот за поддршка на ИКТ.



Електронската пошта е важно средство за комуникација на вработените во Министерството. Се користи за внатрешна и надворешна комуникација.

На вработените силно му се препорачува да не користат било какви комерцијални сметки за електронска пошта при комуникација за службени работи/предмети, бидејќи идентитетот на корисникот не може да биде потврден.

На секоја порака преку електронска пошта од вработените треба да биде прикажана следната порака:

**“ Помогнете да се заштеди хартија - дали е потребно да ја печатите оваа електронска порака?**

ПРЕДУПРЕДУВАЊЕ: Поракава е наменета единствено за лицето или институцијата до која е испратена. Оттаму, истата е строго доверлива и со законски заштитена содржина, чие разоткривање е казниво со закон. Доколку лицето кое ја чита оваа порака не е оној/онаа кому истата му е пратена и/или не е вработен или одговорен за информациите што таа ги содржи, лицето се смета за известно дека е строго забрането било какво неовластено распространување, дистрибуција или копирање на материјалите вклучени во оваа порака. Мислењата и ставовите што ги содржи оваа порака се на нејзиниот автор и истите не секогаш се совпаѓаат со ставот на Министерството за информатичко општество и администрација на Република Македонија. Ниту еден дел од оваа порака ниту од документите прикачени за неа не смее на било каков начин да се употребува или умножува.

Доколку документот сте го примиле по грешка, Ве молиме веднаш за тоа да го известите примателот и да ја уништите пораката.

DISCLAIMER: This message is for the sole use of the person or entity to whom it is being sent. Therefore, it contains strictly confidential and legally protected material whose disclosure is subject to penalty by law. If the person reading this message is not the one to whom it is being sent and/or is not an employee or the responsible agent for this information, this person is herein notified that any unauthorized dissemination, distribution or copying of the materials included in this facsimile is strictly prohibited. Any opinions contained in this e-mail are those of the author of the message and do not necessarily coincide with those of Ministry of Information Society and Administration of the Republic of Macedonia. No part of this message or attachments may be used or reproduced in any manner whatsoever.

If you received this document by mistake please notify immediately to the subscriber and destroy the message.

Потписот треба да биде на македонски и англиски јазик, а треба да ги содржи следните податоци:

“[име и презиме]  
[звање]

[одделение]  
[сектор]  
Министерство за информатичко општество и администрација  
[Адреса]  
[град]  
веб страна.: [www.mioa.gov.mk](http://www.mioa.gov.mk)  
тел.:02.3[...]  
моб.070.3[...] – задолжително само службениот број  
факс: 02.3[...]

Корисниците на електронска пошта -пошта треба често да ја проверуваат содржеината на своето сандаче.

Услугата електронска пошта не смее да се користи за испраќање на застрашувачки или вознемирувачки пораки.

Сметките на електронска пошта се подесени за рутинско локално архивирање на секои 30 дена на пораки постари од 180 дена.

Персоналот за поддршка на ИКТ треба да резервира 1 GB мемориски простор на серверот за сандачето на електронска поштаза секој корисник.

Големината на една порака не може да надминува 10MB.

Услугата е сметките не смее да се користи за несоодветна дистрибуција на:

- труд заштитен со правата на Интелектуална сопственост,
- сексуално експлицитни или непристојни пораки,
- пораки од електронска пошта на друг корисник,
- свесно и злонамерно препраќање на вируси и црви,
- прекршување на закони,
- вознемирувачки пораки исполнети со омраза или закани,
- одговори или проследувања на големи листи на дистрибуција.

## Употреба на Интернет

1. Интернетот е непроценлива алатка за пристапување кон и истражување на информации од различни извори, публикување на податоци од работата на Министерството, користење на е-услуги, комуникација.Вработените мора да се однесуваат одговорно и во согласност со полисата.

Примери на непочитување на оваа полиса се прикажани во продолжение:

- пристапување кон, прикажување на, симнување или ширење на порнографски или други материјали "за возрасни".

- публикување/објавување информации кои можат да имаат тенденција на омаловажување или вознемирување на другите врз база на пол, возраст, боја, национално или етничко потекло, верско уверување, инвалидитет, социјална положба, брачна состојба или сексуална ориентација.
- учество во верижни писма.
- објавување доверливи или информации во сопственост на Министерството, или на било кој од своите деловни соработници на необезбедени интернет локации како огласни табли или ширење на информации кои би можеле да ја нарушат доверливоста на Министерството.
- преземање, користење или дистрибуција на авторски заштитени материјали од интернет без соодветно одобрение од и/или надомест на сопственикот на правата од интелектуална сопственост.
- учество во било каква форма на коцкање.

## 2. Правила на употреба кои се однесуваат на вработените во Министерството :

- Персоналот за поддршка на ИКТ мрежата го задржува правото да ги испитува или брише сите документи што може да се најдат на сметачкиот систем на Министерството или да ги следи сите посетувани интернет сајтови.
- Пристапувањето мора да биде само преку овластена сметка и лозинка, кои не смеат да му бидат на располагање на било кое друго лице;
- Сета интернет употреба треба да биде соодветна на професионална дејност на вработените, со исклучок на "умерена лична употреба, во интерес на рамнотежа помеѓу работата и животот". Банкарски, трговски, eВау, приватна електронски пошта и слични (приватни интереси) веб локации се дозволени во умерени степен, доколку со тоа не се компромитира професионалната употреба на интернетот.
- Забрането е користење на веб локации за социјално вмрежување.
- Забранети се активности кои претставуваат закана за интегритетот на ИКТ системи, или кои напаѓаат или корумпираат други системи
- Корисниците ќе ги препознаат материјалите кои се несоодветни и секое случајно прекршување на правилото треба да го пријават на Државниот секретар.
- Корисници се одговорни за електронска пошта што ја испраќаат, како и за воспоставените контакти кои од што добиваат електронска пошта;
- Истото професионално ниво на јазик и содржина треба да се применува како за писма или други медиуми, со оглед на тоа што пораките по електронска поштасе често проследувани;
- Праќање анонимни пораки и препраќање на верижни писма е забрането;
- Авторското право на материјали и правата на интелектуална сопственост мора да се почитува;

- Користење за лична финансиска добивка, коцкање, политички цели или рекламирање е забрането;
- Дозволена е домашна употреба на преносни копјутери на Министерството, но се забранува пренесување на информации на домашни сметачи, кои содржат лични податоци за ученици или персонал, особено слики и видеа.

3. Корисниците треба да се свесни дека сите интернет врски и пристапи се најавени и мониторирани.

### Полиса за преносни сметачи

Секој преносен сметач е посебно конфигуриран за да му одговара на лицето на кое му е доделен од персоналот за поддршка на ИКТ – систем администраторите. Поради тоа, преносните сметачи не треба да бидат давани на привремено или трајно користење од еден член на вработените на друг без претходна реконфигурација од страна на тимот за поддршка на ИКТ.

Преносните сметачи се во сопственост на Министерството и треба сметачтреба да се чуваат заклучени кога не се во употреба. На крајот на работното време, преносниот сметач треба или да се понесе дома или да се заклучи на безбедно место/фиоки, шкаф итн./

Трошоците за замена и поправка, поради губење или оштетување, ќе ги сноси корисникот на кој му е доделен преносниот сметач, доколку губењето/оштетувањето настанали под следните околности:

- преносниот сметач е заборавен во автомобил,
- преносниот сметаче заборавен во канцеларија/хотел/сала за состаноци и не заклучен на безбедно место во текот на ноќта,
- преносниот сметач паднал на земја,
- преносниот сметачт прегреал,
- други причини предизвикани од невнимателно или погрешно однесување од страна на корисникот на кој му е доделен преносниот сметач.

Вработените на кој им е доделен преносниот сметачна користење не смеат сами да вршат интервенции на конфигурацијата на истиот.

### Телефони

Телефоните и телекомуникациската опрема и услуги обезбедени од Министерството служат како алатка при извршување на службените активности. Приватни телефонски повици во работно време, вработените можат да примаат/вршат во разумен обем и граници.

## Одржување и безбедност на веб-локацијата на Министерството

Министерството самото ја хостира сопствената Веб-страна, при што:

- Персоналот за поддршка на ИКТ е одговорен за сите позадински операции за веб-локацијата, како: работа на сервер, хостирање на софтвер, безбедност и враќање од катастрофи, и друго потребно за веб-локацијата да е постојано достапна и функционална.
- Кабинетот на министерот е одговорен за одржување на содржината на веб-локацијата.
- Назначено е лице од персоналот за поддршка на ИКТ е одговорно на ажурирање на содржината на веб локацијанта на Министерството
- Одговорност на персоналот за поддршка на ИКТ е да одржува резервни копии на веб содржините. Резервна копија од целата страна се прави секоја вечер.

## Ревизија на софтвер и хардвер

Министерството има обврска да се осигура дека само легален софтвер се користи на опремата во негова сопственост.

Државниот секретар ќе биде известен за било каков нелегален софтвер откриен при процесот на увид на сметачите..

## Преместување на опрема

Опрема или други средства за електронски комуникациски не смее да се позајмува, отстранува или преместува од одредена локација, без експлицитна дозвола на министер/ Државниот секретар.

Освен преносливата опрема наменета за користење надвор од Министерството, ниту една друга опрема не може да се изнесе од просториите на Министерството без експлицитна дозвола на Државниот секретар. За да се добие дозвола, мора да се пополнат неопходните формулари, дефинирани во процедурите за МІОА 202-Р1 Доделување информатичка опрема и пристап до ИТ ресурсите.

## Резервни копии и враќање на податоците

- Персоналот за поддршка на ИКТ е одговорен за обезбедување на враќањето на податоци од катастрофи за сите податоци на мрежните сервери на Министерството.
- Министерството моментално ја спроведува политика на креирање системска резервна копија на мрежата согласно донесеното упатство за управување со резервни копии на податоци (backup) во министерството за информатичко општество.
- За изготвување резервни копии на сите локални системи, исклучиво е одговорен секој корисник за сопствените податоци. Персоналот за поддршка на ИКТ не е одговорен за било каква загуба на податоци направени на локалниот систем поради оштетувања во системот, кражба или нарушувањата на безбедноста.
- Соодветни периферни уреди за подготовка на резервни копии, на пример: CD режач, USB диск, итн. ќе бидат обезбедени за секој корисник на негово барање. Рутинското складирање и безбедност на сите архивирани податоци на локалниот систем е одговорност на секој корисник.
- Доколку системски диск сметачот треба да се форматира или замени, Персоналот за поддршка на ИКТ ќе се обиде да ги врати и реставрира папката "My Documents", на Internet Explorer "My Favorites" датотека, "Microsoft Outlook", "Address Book", како и електронската пошта. Персоналот за поддршка не го гарантира враќањето и интегритетот на сите податоци што ќе се обиде да ги спаси.
- Сите медиуми за резервни копии и документираните процедури за нивно изготвување, ќе бидат чувани на безбедно место согласно донесеното упатство за управување со резервни копии на податоци (backup) во министерството за информатичко општество.
- Резервните копии ќе бидат предмет на рутински квалитативни тестови за обезбедување на интегритетот на архивираните податоци.

## Сервери и ажурирање на безбедноста на локалните системи

Сите мрежни сервери и локалните системи се распоредени за дневни ажурирања од страна на Персоналот за поддршка на ИКТ мрежата. или, односно се мисли ли на: дневните ажурирања на сите мрежни сервери и локалните системи се распоредени на ПП.

Откако ќе бидат превземени, надградбите автоматски се инсталираат на серверите и на локалните системи.

## Анители - Вирусна полиса и процедура

- Сите сервери и локалните системи поставени на мрежата на Министерството се обезбедени со анти-вирус софтвер, купен од страна

- на Министерството.
- Анти-вирус софтверот вклучува "ажурирање во живо", кое врши неделни симнувања на најновите вирус-дефиниции, за да се обезбеди заштита од црви и вируси.
  - Вработените во министерството, доколку откријат вирус или црв на сервер или на локален систем, инфицираниот елемент веднаш се симнува од мрежата, се врши проценка, чистење, а потоа и тестирање.
  - Ако се утврди дека вирус или црв не може да се отстрани од системот, заразениот диск се реформира, се инсталира соодветен оперативен систем и на сметачот се реставрира соодветната најнова резервна копија на податоци.
  - Откако ќе се утврди дека системот не е повеќе закана за мрежата на Министерството, сметачот ќе биде интегриран назад во мрежата на Министерството.

### **Физичка безбедност**

- Политика на Министерството е да се чуваат заклучени и обезбедени од јавен пристап сите сервери, рутери, свичеви, и друга опрема од клучно значење за мрежата.
- Клучевите од објектите во кои се поставени мрежни сервери и уреди се под надзор на персоналот за поддршка.
- Сите земени клучеви од страна на овластени лица од персоналот за поддршка на ИКТ мрежата, се враќаат кај службата за обезбедување на објектот.
- Пристапот до целиот позадински хардвер од клучно значење за мрежата на Министерството е дозволен само на персоналот за поддршка.
- Сите лица кои неовластено вршат било какви нагудувања на било кој мрежен системски уред како сервери, рутери, итн. ќе се смета дека ја прекршуваат безбедноста на мрежата, и за спречување ќе бидат преземени соодветни активности. Вработените во Министерството треба да ги пријавуваат сите прекршувачки пристапувања на било кој од мрежните системи и уреди.
- За физичката безбедност на персоналните системите на вработените е одговорен секој вработен поединечно, особено за систем отстапен на користење. Сите сметачи треба да останат во просториите во кои се инсталирани/поставени.
- Одговорност на секој корисник е да го контактира персоналот за поддршка во случај на кражба или оштетување на десктоп систем.

### **Процедури за системско тестирање**

Поради чувствителната природа на информациите во Министерството, персоналот за поддршка воспоставува полиси чија цел е да ги задржи целиот хардвер и софтвер за развој и тестирање одвоени од пристапната мрежа. Хардверот и софтверот кои се клучни за функционирањето на Министерството мора да се одржуваат изолирано од тестна / развојна околина, за да се спречи случајно корумпирање на активните системи, да се спречи пристап до тестните системи од страна на неовластени корисници на мрежата, како и можен губиток и корупција на важни податоци.

- Софтверот чие тестирање е во тек треба да се имплементира на самостоен систем, со свој сопствен процесор, дискови, и со пристап ограничен на назначени поединци.
- Системи кои содржат компајлери, код, и системски единици не треба да бидат достапни на активните системи.
- Лицата назначени за тестирање и развој на системи, за таа намена треба да користат имиња и лозинки различни од оние со кои рутински пристапуваат до активниот систем.
- Одобрување за подигање на тест систем за оперативен пристап мора да биде дадено од страна на Министерот/ Државниот секретар, а по предлог и образложение дадено од проектен координатор во Министерството.

## ОТСТРАНУВАЊЕ НА СТАРА ОПРЕМА

### Вовед

Честите промени на ИТ околината подразбира дека сметачска опрема (персонални и префиррерни сметачи, и периферни уреди како што се печатачи) периодично застарува, дотрајува или станува вишок на потребите. Вообичаена пракса е таквите сметачи и друга опрема да се пренесуваат во други владини институции / организации (пренасочување), да се продаваат на аукција или да се донираат на добротворни организации или едноставно да се исфрлат.

### Полиса

#### Опции за отстранување на ИТ опрема

Кога стануваат излишни, со сметачите се постапува според следната приоритетна листа:

- Повторно пуштање во употреба во друга владина институција / организација.
- Донација на добротворна организација, која мора да гарантира дека ќе ја користи истата
- Продажба на аукција.
- Исфрлање.



## Отстранување на податоци и софтвер

Сите траги на податоците содржани на сметачската опрема мора да бидат отстранети и уништени од страна на персоналот за поддршка, пред опремата да биде отстранета. Обичното бришење на документот или реформатирањето на хард дискот не ги отстранува трагите на сите податоци и не го оневозможува нивното враќање. За комплетно бришење на целата содржина на дискот, потребно е да се користат специјализирани техники/алатки.

## Procedures – процедури

### Реактивација на сметач во друга владина институција / организација

Освен ако примателот има деловно барање за пренос на некои од податоците, персоналот за поддршка мора да ги отстрани сите податоци од сметачот. Софтверот или лиценците може да се задржат или да се пренесат на новиот сопственик единствено ако постои деловно барање за пренос на лиценцата.

Донирање на излишна сметачска опрема се врши само со одобрување од министерот, при што потребно е да се запази соодветната законската процедура.

### Донирање на надворешна институција

Донирање на излишна сметачска опрема се врши само со одобрување од министерот, при што потребно е да се запази соодветната законската процедура.

Целиот софтвер и сите податоци мора да бидат безбедно отстранети со користење на специјални средства.

Лиценциран софтвер на Министерството може да се задржат или да се пренесат на новиот сопственик единствено ако постои деловно барање за пренос на лиценцата.

Персоналот за поддршка – администраторите треба да обезбеди дека примателите на сметачската опрема мора да се известени дека Министерството не ја гарантира безбедноста или погодноста на опремата и истото се оградува од секаква одговорност за нејзино одржување.

Треба да се води евиденција за сметачката опрема донирана на трети лица, како доказ дека Министерството, онаму каде што е тоа возможно и има

смисла, се грижи за зголемување на стапката на рециклирање на индустриски материјали.

### Одлагање на опремата на еколошки прифатлив начин

Постарите монитори се сметаат за опасен отпад и нивното исфрлање мора да се организира согласно соодветниот закон за електронски отпад преку овластена компанија.

### **Техничка поддршка на корисници**

Со цел да се подобри функционирањето на ИКТ системот во Министерството како и целокупната техничка поддршка на корисници, од страна на персоналот за поддршка се формира група која дава техничка поддршка на корисниците. Барањата за техничка поддршка или за решавање на едноставни проблеми, корисниците на системот ги доставуваат на [it\\_helpdesk@mioa.gov.mk](mailto:it_helpdesk@mioa.gov.mk)

### **Споделување на податоци**

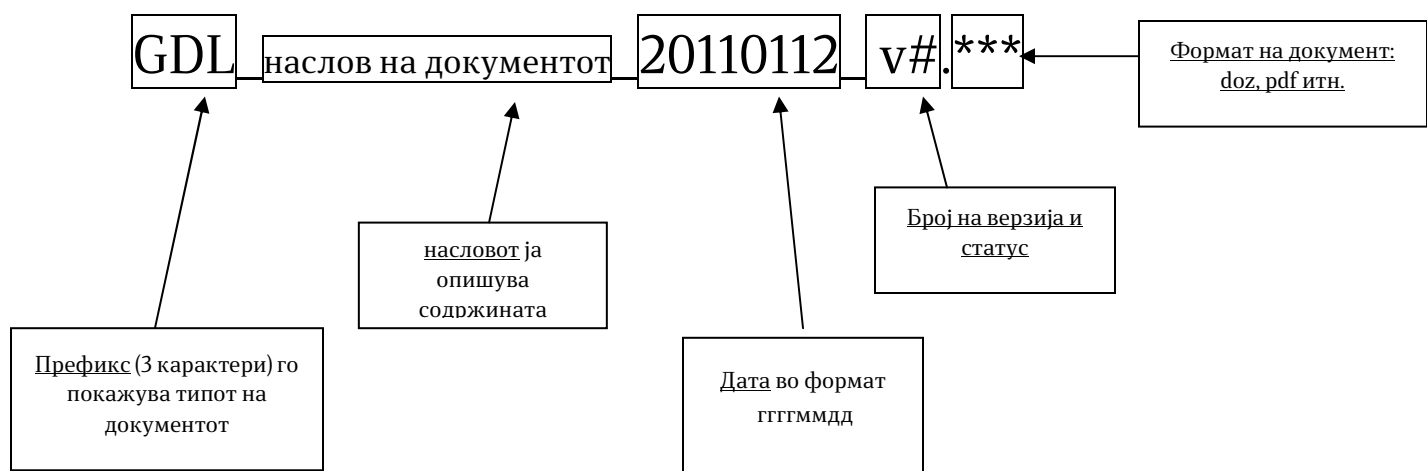
Во рамки на Министерството, корисниците можат да споделуваат документи преку:

- Комуникација преку електронска пошта.
- Документи на "mioshare" – простор на серверот предвиден за споделување, со предефинирана структура на папки која соодветствува на проектната поставеност.

Spark – единствениот одобрен P2P клиент за споделување на пораки и датотеки, инсталиран на секоја работна станица во мрежата на Министерството.

## Конвенција за именување на документи

Имињата на документите креирани од корисниците, се состојат од четири дела споени со карактерот „долна црта“ (\_). Името на документот не треба да содржи празни места.



Деловите на конвенција за именување се:

- Префикс кој покажува каков тип на документ е датотеката, (3 карактери, големи букви, опишан во табелата подолу),
- Насловот на документот кој ја опишува содржината, (максимум 20 карактери, мешани букви и цифри, без празни места),
- Датумот кој покажува кога е создаден, ( 8 карактери, цифри, без празни места), и
- Бројот на верзијата и статусот на документот (максимум 4 карактери, големи букви, опционо).

КОД	Опис
AGD	Агенда
AGR	Согласност
ASS	Проценка
BGT	Буџет
COR	Надворешна кореспонденција
EVL	Оценка
GDL	Насоки
GOV	Владини материјали
INS	Инструкции
LEG	Законодавство
MAN	Прирачник
MEM	Меморандум – внатрешна комуникација

<b>MIN</b>	Минути и белешки – Белешки од состаноци и тел. разговори (формални/неформални)
<b>ORG</b>	Организационен дијаграм
<b>PLN</b>	План
<b>POL</b>	Полиса
<b>PRO</b>	Процедура
<b>PRP</b>	Проект
<b>PUB</b>	Публикации за меѓународни и промотивни цели, вклучително билтени
<b>REP</b>	Извештај
<b>SPC</b>	Спецификација
<b>TDO</b>	Тендерска документација
<b>TEM</b>	Урнек
<b>TRE</b>	Обука

### **Чувствителни информации**

Министерството има законска обврска да ги штити чувствителните информации на вработените, нивните лични податоци, како и податоци на/за клиентите согласно закон.

Чувствителните информации мора да се чуваат на стриктни локации и само на персонални работни станици.

Чувствителните информации не смее да се снимаат или копираат на заедничка споделена локација, ниту пак да им се извршува трансфер преку електронска пошта или Spark.

### **Користење на фонтови**

Вработените во Министерството, како за кореспонденција така и за внатрешна комуникација треба да ги користи StobiSerif Regular и StobiSerif Bold, големина 11.