Безбедносна политика на Агенцијата за аудио и аудиовизуелни медиумски услуги во областа на информациско-комуникациската технологија (Пречистен текст)

**Вовед и цел:**

Овој документ овозможува преглед на безбедносната политика на Агенцијата за аудио и аудиовизуелни медиумски услуги во областа на информациско-комуникацискатa технологија (ИКТ), процедури, прирачници, упатства и водичи. Овие политики се од голема важност за безбедноста на ИКТ системот на Агенцијата за аудио и аудиовизуелни медиумски услуги (ААВМУ), и истите се наменети за заштита на самите корисници, податоците и интелектуалната сопственост на ААВМУ. Процедурите во овие политики се за заштита на ИКТ ресурсите, податоците и интелектуалната сопственост на Агенцијата.

Секторот за информатичка поддршка и општи работи, односно Одделение за информатичка поддршка и технологии е на мислење дека со воспоставување и континуирано надградување на системот за управување со ИКТ безбедност би ги применувала барањата на ISO 27001:2005 стандардот.

Во продолжение наведени се законите кои се применуваат а кои се однесуваат на ИКТ безбедност за податоците во електронска форма, електронски потпис, класификација на информации, слободен пристап до информации.

- Закон за електронски комуникации, („Службен весник на Република Македонија" бр.13/05, 14/07, 55/07, 98/08, 56/09, 83/10, 171/10, 13/12, 59/12, 123/12 и 23/13)
- Закон за следење на комуникациите ("Службен весник на Република Македонија" бр. 121/06, 110/08 и 4/09)
- Закон за податоците во електронски облик и електронски потпис ("Службен весник на Република Македонија" бр. 34/01, 6/02 и 98/08)
- Закон за електронско управување ("Службен весник на Република Македонија" бр. 105/09)
- Закон за заштита на личните податоци, („Службен весник на Република Македонија" бр.7/05, 103/08, 124/08, 124/10 и 135/11)
- Закон за класифицирани информации ("Службен весник на Република Македонија" бр. 9/04 , бр.113/07, бр. 145/2010, бр. 80/2012 и 41/2014)
- Закон за слободен пристап до информации од јавен карактер („Службен весник на Република Македонија" бр.13/06, 86/08 и 6/10)
- Правилник за технички и за организациски мерки за обезбедување тајност и заштита на обработката на личните податоци ("Службен весник на Република Македонија" бр. 38/09)

**Опсег:**

Оваа политика се однесува на сите корисници на ИКТ системот на Агенцијата за аудио и аудиовизуелни медиумски услуги. Корисници се дефинирани како поединци со авторизиран пристап до информациско-комуникациските ресурси на Агенцијата за аудио и аудиовизуелни медиумски услуги, вклучувајќи ги и вработените лица на одреден временски период и другиот персонал, како лица кои се со посебни договори за работа, изведувачи на проекти, консултанти и сите останати странки (физички и правни лица) кои имаат валидни кориснички овластувања.

**Политика:**

Информациите се критично добро на Агенцијата за аудио и аудиовизуелни медиумски услуги и мора да бидат соодветно заштитени од неавторизиран пристап до истите, заштита од бришење или уништување и модификации, намерни или ненамерни од страна на корисниците.
Сите учесници во ИКТ системот на ААВМУ имаат соодветна улога во заштитата и безбедноста на овие добра. Вработените, привремено вработените, лицата со ограничен работен временски рок, изведувачите и консултантите и сите други странки кои имаат пристап до ИКТ средствата сопственост на ААВМУ се одговорни за да партиципираат во безбедноста на овие добра. Секторот за информатичка поддршка и општи работи треба да создаде процедури за креирање на безбедна околина преку имплементација на политики со дефинирани улоги и одговорности и овозможување на конзистентна координација.
На вработен во Агенцијата за аудио и аудиовизуелни медиумски услуги на кој му престанува работниот однос, строго се забранува бришење на службените податоците кои ги располагал додека бил работно ангажирани во Агенцијата, форматирање на персоналниот компјутер кој го користел или бришење на службениот е-маил кој му бил доделен од страна на Агенцијата.

**Одговорност:**

- ✓ Секој корисник е одговорен за спроведување на пропишаните политики за безбедност на информациите.
- ✓ Раководителите на сектори се должни да обезбедат дека вработените во нивните сектори ги спроведуваат политиките за безбедност на информации.
- ✓ Секој корисник кој ќе увиди дека се случил упад во системите или се создаваат вакви услови има должност и мора да ги извести раководителот на секторот, раководителот на Сектор за информатичка поддршка и општи работи кој потоа го известува Директорот / Заменикот на директорот на Агенцијата.

**Изјава за политика (POLICY STATEMENT)**

"Сектор за информатичка поддршка и општи работи на Агенцијата за аудио и аудиовизуелни медиумски услуги ќе обезбеди адекватна заштита и доверливост на податоците и сопствениот софтверски систем, без разлика дали тие се наоѓаат на централно или локално ниво и ќе го обезбеди интегритетот на податоците, за конфигурациите и програмите преку обезбедување на континуиран пристап на сите авторизирани корисници на ИКТ системот на Агенцијата за аудио и аудиовизуелни медиумски услуги."

## 1. ГЛАВНИ БЕЗБЕДНОСНИ ПОЛИТИКИ

1.1. Доверливоста на податоците на Агенцијата за аудио и аудиовизуелни медиумски услуги ќе биде одржувана преку контрола на пристап (физичка и логичка), и во согласност со соодветна класа на функционална сигурност.

1.2. Интернет пристапот нема посебни ограничувања и е достапен за сите корисници.

1.3. Само авторизиран и лиценциран софтвер може да биде инсталиран на системите, а самата инсталација ќе биде изведена од претставници на Сектор за информатичка поддршка и општи работи на Агенцијата –Одделението за информатичка поддршка и технологии или од лица со соодветни овластувања (економски оператори со кои постои соработка во областа на ИТ).

1.4. Користењето на неавторизиран софтвер е забрането. Во случај да биде откриен неавторизиран софтвер тој ќе биде веднаш отстранет од работната станица.

1.5. Сите мемориски уреди, дискови и други типови на преносни медиуми од надворешни извори мора најпрвин да се проверат дека се безбедни за користење и дека не се инфицирани од вируси пред воопшто да се користат во ИКТ системот на Агенцијата за аудио и аудиовизуелни медиумски услуги, прво со проверка со софтверско антивирусно решение, а ако е потребно да се бара и асистенција од Сектор за информатичка поддршка и општи работи- Одделение за информатичка поддршка и технологии.

1.6. Лозинките мора да се конструираат како композиција од алфанумерички карактери и специјални знаци (минимум 8 карактери) и мора да се менуваат периодично, како што е дефинирано во процедурата за доделување и ракување со лозинки.

1.7. Конфигурирањето на работните станици може да биде единствено изведено од претставници на Сектор за информатичка поддршка и општи работи - Одделението за информатичка поддршка и технологии или од лице со соодветно овластување. Само лице од Секторот за информатичка поддршка и општи работи- Одделението за информатичка поддршка и технологии или друго овластено лице може да врши (ре-) инсталација на опрема и поврзување во компјутерската мрежа.

1.8. Доделувањето на IP адреси на опремата може единствено да биде изведено од претставници на Сектор за информатичка поддршка и општи работи или од лице со соодветно овластување. Претставници на Сектор за информатичка поддршка и општи работи го конфигурира серверот за динамично доделување на адреси (Dynamic Host Configuration Protocol - DHCP) за оваа намена.

1.9. За да се спречи загуба на податоци и/или застој во работата и да се предизвика нарушување на надлежноста на системот, претставници на Секторот за информатичка поддршка и општи работи- Одделението за информатичка поддршка и технологии треба да преземат мерки за заштита на податоците, апликациите, конфигурациите на работните станици и серверите и другите софтвери на други медиуми.

## 2. ФИЗИЧКИ МЕРКИ ЗА ЗАШТИТА

2.1. Примарната локација на главниот компјутерски центар мора да биде во објектот на Агенцијата за аудио и аудиовизуелни медиумски услуги во посебна заштитена и обезбедена просторија. Доколку Агенцијата донесе политика да формира регионални центри тогаш тие простории треба да бидат заштитени, но со пониско ниво на сигурност.

2.2. Просторијата во која е поставен главниот компјутерски систем (сервер сала) треба да биде заклучена просторија дури и кога е напуштена / празна.

2.3. Постојан влез во сервер салата имаат лицата со овластување од Директорот на Агенцијата.

2.4. Пристапот на други лица во сервер сала е овозможен само во придружба на овластените лица од претходната точка (2.3).

2.5. Времето на влез и излез во сервер салата го евидентира работник од Сектор за информатичка поддршка и општи работи односно одделението за информатичка поддршка и технологии, определен од Раководителот на Секторот.

2.6. Регулатор на температура со соодветен систем за противпожарна заштита е неопходно да биде воспоставен во сервер сала заради заштита на опремата првиот систем од прегревање, а вториот заради заштита од пожари.

2.7. Мора да се обезбеди најдобра изолација од влага.

2.8. Подот на сервер салата треба е изграден од метална решетка подигнат до 50 цм, прекриен со антистатички панели кои може да се креваат. Тоа ќе овозможи да во случај на поплава првин се поплавува тој дел и ќе се заштити опремата, а второ таквата изведба треба да овозможи сите кабли низ сервер салата кон и од системите лоцирани таму бидат под-подно положени.

2.9. Соодветни сензори за движење треба да бидат воспоставени со алармен систем за тревожење при неовластено движење на лице во компјутерскиот центар.

2.10. Доколку е возможно, компјутерската опрема да се чува на минимум 1.5м растојание од отворен прозор. Просторијата да е опремена со соодветен систем за следење на движење (систем за видео надзор).

2.11. Опремата која има систем за физичко заклучување задолжително да се заклучува кога не е во функција.

2.12. Сервер салата е сместена во близина на канцелариите на Одделението за информатичка поддршка и технологии, согласно нормите за сервер сала..

2.13. Целокупната серверска опрема мора да биде лоцирана во сервер сала, монтирана во соодветни метални ормари (анг. rack), како и активната мрежна опрема која е лоцирана како во сервер сала така и низ другите објекти од кампусот, со обезбеден уред за непрекинато напојување (анг. Uninterruptible Power Supply – UPS).

2.14. Целокупната серверска опрема треба да биде приклучена на соодветни уреди за непрекинато напојување кои во случај на испад или прекин на електрична енергија ќе извршат безбедно задржување во оперативна функција и спуштање на серверите при подолготраен прекин.

2.15. Опремата која е на располагање на корисниците на системот во случај кога се отсутни од работното место вон работно време треба да биде исклучена. Во работно време зависно од отсуството ако е подолго од 1 час треба да се исклучи, ако не треба корисникот да ги затвори сите програми и да се одјави од систем или софтверски заклучи.

2.16. Кога корисниците на опремат се отсутни подолго од 1 ден, опремата која ја користат треба да биде исклучена и од електричното напојување.

## 3. ЗАШТИТА ОД ВИРУСИ, УПАДИ И ДРУГИ НЕПРАВИЛНИ ПАКЕТИ ОД МРЕЖАТА

3.1. Агенцијата за аудио и аудиовизуелни медиумски услуги обезбедува заштита од вируси, упади и неправилни пакети на два нивоа. Првиот ниво на заштита се остварува преку router-firewall (CISCO ASA), кој врши заштита од упади, лоши пакети и други неправилности во мрежниот сообраќај.

3.2. Второто ниво на заштита се остварува преку софтверските решенија за заштита од вируси кои се инсталираат на работните станици, сервери, преносни компјутери и друга опрема која пристапува во мрежата на Агенцијата за аудио и аудиовизуелни медиумски услуги и Интернет. Софтверското решение треба да биде доверливо, активен и со ажурни дефиниции, способен за спречување на вирусни активности.

3.3. Податочните сервери ќе бидат заштитени со софтвер за скенирање од компјутерски вируси.

3.4. Сите работни станици периодично ќе се скенираат од компјутерски вируси.

3.5. Сите податочни дискови или уреди со потекло надвор од Агенцијата, можат да биде користени откога ќе бидат поставени и тестирани во просториите на Сектор за информатичка поддршка и општи работи. Софтверите за скенирање треба редовно да се ажурираат.

3.6. Сите системи ќе бидат изградени од оригинални, чисти мастер копии кои секогаш биле заштитени за дополнително запишување на истите. Оригиналните мастер копии ќе бидат користени само при претходно скенирање од вируси на истите.

3.7. Сите преносни мемориски медиуми што содржат егзекутабилни софтвери (софтвери со екстензии од типот: .exe или .com) мора да бидат заштитени од дополнителни запишувања на истите.

3.8. Сите презентации и софтверски демонстрации од добавувачи треба да биде изведени на нивна опрема и не треба да се поврзуваат на инфраструктурата од Агенцијата

3.9. Не се дозволува користење на демо и пробни софтвери, кои се симнати од интернет или дистрибуирани на други медиуми. Доколку е неопходно користењето на овој вид на софтвери тогаш претходно треба да се обезбеди дека софтверот не е извор на компјутерски вирус.

3.10. Нов софтвер ќе биде скениран од компјутерски антивирус од страна на претставник на Сектор за информатичка поддршка и општи работи пред да биде инсталиран и ставен во функција.

3.11. Сите дискови со податоци од надворешни лица или персонал од теренска работа пред да бидат преснимени или ставени во функција треба да бидат проверени дека нема присуство на вируси.

3.12. За да се овозможи податоците да бидат реставрирани во случај на напад од инфекции од вируси, се врши редовна заштита на податоците на други медиуми .

3.13. Менаџментот треба да ги презеде сите неопходни мерки за спроведување на заштита од вирус, спајвер и спречување на упади.

3.14. Корисниците треба редовно да се информирани за тековните политики и процедури за заштита од вирус, спајвер и спречување на упади.

3.15. Корисниците ќе бидат известени за инциденти предизвикани од вируси, спајвери и упади во ИКТ системот на Агенцијата.

3.16. Вработените ќе бидат одговорни за прекршувања на политиките пропишани во врска со употребата и функционирањето на софтверите за заштита од вирус, спајвер и спречување на упади.

3.17. Политиките и процедурите за софтверите за заштита од вируси, спајвер и спречување на упади ќе бидат редовно проверувани и доколку треба ажурирани според нови услови.

3.18. Во случај на веројатна вирус инфекција , спајвер или упад во системот претставници на Сектор за информатичка поддршка и општи работи мора веднаш да биде известен. Претставникот од секторот ќе ја изолира инфицираната машина и изврши скенирање на сите дискови и сите други работни станици на кои вирусот можел да се пренесе.

## 4. ДОЗВОЛИ ЗА ПРИСТАП

4.1. Компјутерскиот мрежен систем во Агенцијата за аудио и аудиовизуелни медиумски услуги користи архитектура со централно најавување – активен директориум (Active Directory). Корисниците во мрежата имаат различни улоги и привилегии.

4.2. Секторот за информатичка поддршка и општи -Одделението за информатичка поддршка и технологии работи мора да биде известен од соодветниот секторот за нов вработен за да отвори корисничко име. На корисниците ќе им бидат доделени толку права и привилегии во информатичкиот систем, доволни за нормално изведување на секојдневните работни обврски според дефинираните права. Корисничките права и привилегии постојано ќе се одржуваат на минимум.

4.3. За различни сектори се дефинира различно ниво на пристап до одредени ресурси од податоците на Агенцијата. Доколку некој вработен во Стручната служба има потреба од пристап до дополнителни ресурси, раководителот на секторот во кој припаѓа вработениот треба да достави писмено барање до Директорот на Агенцијата.

4.4. Секторот за информатичка поддршка и општи работи ќе врши контроли на мрежните / серверски лозинки и истите ќе бидат доделени од систем администратор. Систем администраторот е одговорен за одржување на интегритетот на податоците на корпоративните системи и за привилегиите за пристап на корисниците.

4.5. Пристапот до информатичките ресурси и серверски системи ќе се остварува преку индивидуални единствени кориснички овластувања (имиња) и лозинки.

4.6. Корисничките имиња и лозинките не треба да се споделуваат со другите корисници.

4.7. Корисничките имиња и лозинките не треба да бидат испишани кај корисниците.

4.8. Корисничките имиња се конструирани од првата буква на името и целото презиме одвоени со точка, или името и презимето одвоени со точка на корисникот

4.9. Сите корисници имаат алфанумерички лозинки со минимална должина од карактери.

4.10. Лозинките ќе станат невалидни после 90 дена и треба да се променат. Тие се единствени и уникатни.

4.11. Систем за детекција од упади во системите ќе биде воспоставен доколку тоа е возможно. Корисничкото име ќе се заклучи во случај на 3 неуспешни обиди за најава со истото.

4.12. На корисниците ќе им бидат доделени корисничките имиња и лозинките за најава на локалната мрежа за користење на ИКТ ресурси додека за најава на други индивидуални системи ќе се користат други лозинки.

4.13. Сектор за информатичка поддршка и општи работи мора да биде известен од правната служба за секој еден вработен кој привремено или трајно го напушта работењето во Агенцијата за аудио и аудиовизуелни медиумски услуги. Претставници на Секторот за информатичка поддршка и општи работи веднаш ќе изврши одземање на привилегиите за пристап на системот со исклучување/бришење на корисничкото име.

4.14. LAN / серверските администраторските лозинки ќе се чуваат и во хартиена форма затворени во коверт, печатен од надвор, а ќе се чуваат заклучени кај раководителот на Секторот за информатичка поддршка и општи работи, за во случај на многу итни непланирани ситуации.

4.15. Ќе се имплементира систем на следење на бројот на неуспешни обиди за најава на систем, успешни најави и измени причинети од корисниците.

4.16. Употребата на администраторските и супервизирските акаунти треба да биде сведено на минимум.

4.17. Лозинките доделени на системите по подразбирање при инсталација (default лозинките) мора веднаш да се променат после инсталацијата.

## 5. ОБЕЗБЕДУВАЊЕ НА МРЕЖА

5.1. Активната мрежна опрема (свичеви, рутери, модеми и др.) ќе биде поставена во заклучени метални ормари. Пристапот до овие уреди единствено е дозволен на претставници на Сектор за информатичка поддршка и општи работи - Одделението за информатичка поддршка и технологии и доколку има други надворешни овластени лица, кои во случај на интервенција задолжително треба да го известат одговорниот од Сектор за информатичка поддршка и општи работи.

5.2. Мрежни дијаграми за поставеноста на пасивната мрежна опрема и интерконекциите целосно треба да бидат документирани.

5.3. Периодични проверки и тестирања ќе се прават на мрежните кабли кои се дел од пасивната мрежна опрема во Агенцијата за аудио и аудиовизуелни медиумски услуги.

5.4. Таму каде има потреба, ќе бидат положени редундантни мрежни линкови.

5.5. Користење на софтвери за скенирање на мрежни параметри и мрежни активности смее да користи само претставници од Сектор за информатичка поддршка и општи работи.

5.6. Софтверите за скенирање на мрежа ќе се чуваат во обезбедена просторија кога тие не се користат.

## 6. WAN БЕЗБЕДОНОСНИ МЕРКИ

6.1. Користењето на модеми треба да биде крајно рестриктивно.

6.2. Сите активни уреди кои вршат рутирање на пакети како рутери и/или свичеви треба да се чуваат на обезбедени заклучени места недостапни за корисниците.

6.3. Сите непотребни протоколи за комуникација и комуникациски порти кои постојат на рутерите треба да бидат исклучени.

6.4. Постојаните конекции кон интернет и кон други надворешни мрежи (изнајмените линии) треба да се заштитени со соодветен заштитен ѕид (firewall) за регулирање на мрежниот сообраќај.

6.5. Сите непотребни сервиси и протоколи за комуникација на firewall уредите ќе бидат исклучени.

6.6. Мрежната опрема ќе биде конфигурирана за исклучување на неактивните сесии.

6.7. Сите корисници нема да може директно на пристапат на интернет, мора интернет конекциите да бидат заштитени од неовластен надворешен упад.

**Прилог 1**

**Процедура за доделување и ракување со лозинки**

## Политика на лозинки на Агенцијата за аудио и аудиовизуелни медиумски услуги

### Вовед

Лозинките се важен аспект на компјутерската сигурност. Тие се основна заштита на корисничкиот пристап. Лошо избрана лозинка може да резултира со компромитирање на целата мрежа на Агенцијата за аудио и аудиовизуелни медиумски услуги. Затоа, сите вработени во Агенцијата за аудио и аудиовизуелни медиумски услуги се одговорни во преземање соодветни чекори, како е наведено подолу во текстот за да ги одберат и заштитат своите лозинки.

### Цел

Целта на оваа процедура е воспоставување стандард за креирање строги лозинки, заштита на овие лозинки и фреквенција на нивни промени.

### Обем

Политиката ги вклучува сите вработени кои имаат или се одговорни за корисничко, компјутерско овластување (или било каква друга форма на пристап која поддржува или бара лозинка) , на било кој систем во просториите на Агенцијата за аудио и аудиовизуелни медиумски услуги, има пристап до компјутерската мрежа на Агенцијата за аудио и аудиовизуелни медиумски услуги, или чува било каква интерна (не-јавна) информација во Агенцијата за аудио и аудиовизуелни медиумски услуги.

### 1.0 Политика

#### 1.1 Генерално

- Сите лозинки на системско ниво (пр. Windows Server администрација- ОС администрација, лозинки на администрација на апликации и проекти...) мора да се менуваат барем квартално.
- Целата продукција на лозинките на системско ниво мора да се дел од базата на податоци за администрирање и следење на лозинките.
- Сите лозинки на корисничко ниво (пр. електронска пошта, web, персонален компјутер...) мора да се менуваат на 90 дена.
- Корисници кои имаат привилегии на системско ниво, делегираат и управуваат со овластувањата, преку групната припадност во секторот или одделението или според овластен пристап до заеднички документи и програми. Тие мораат да имаат единствена лозинка за сите корисници.
- Лозинката не смее да се вметне во електронска порака или друга форма на електронска комуникација.
- Сите лозинки на корисничко и системско ниво мора да се издадени според упатствата дадени подолу.

#### 1.2 Упатства

**А. Упатства за конструкција на лозинки**

Лозинките се користат за различни намени во Агенцијата за аудио и аудиовизуелни медиумски услуги , а најчесто за: кориснички овластувања до мрежните ресурси, документи и апликации, web овластувања, email овластувања, screen saver заштита и пријавување на уреди за комуникација (рутер, концентратор,модем...). Сите треба да бидат свесни за тоа како да одберат строга лозинка.

Едноставна , слаба лозинка ги има следните карактеристики:

- Лозинката содржи помалку од осум карактери .
- Лозинката е збор во речник (македонски или странски).
- Лозинката е често користен збор како:
  - ✓ име во семејство, галениче, пријател, колега,...
  - ✓ Компјутерски термини и имиња, команди, компании, hardware, software.
  - ✓ Зборови како "Агенцијата за аудио и аудиовизуелни медиумски услуги", "администрација", име на служба или било каква деривација.

- ✓ Родендени и други персонални информации како што се адреси и телефонски броеви.
- ✓ Низа од букви и бројки како што се aaabbb, qwerty, zyxwvuts, 123321, итн.
- ✓ Било кои од горенаведените напишани наопаку.
- ✓ Било кои од горенаведените со брока во префикс или суфикс (пр., secret1, 1secret)

Строга лозинка ги има следните карактеристики:

- Содржи и мали и големи букви (пр., a-z, A-Z).
- Содржи бројки и знаци на интерпункција како и букви (пр., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
- Да биде со должина од барем осум алфанумерички карактери.
- Да не биде збор од било кој јазик , дијалект,наречје, жаргон, итн.
- Не се базира на персонална информација, имиња во семејство, итн.
- Лозинките не треба никогаш да се запишат на хартија или чуваат on-line. Обидете се да креирате лозинки кои можат лесно да се запомнат. Еден начин за креирање лозинки е базирана на назив на песна, афирмација или друга фраза. На пример, фраза може да биде: "Ова е еден можен начин за помнење" и лозинката може да биде: "Oe1mNzP!" или "Oe1mN>p~" или некоја друга варијација.

***ЗАБЕЛЕШКА: Не користете ни еден од овие лозинки !***
***За да ја проверете строгоста на лозинката тоа може да го направите во сајтот : http://www.microsoft.com/protect/yourself/password/checker.mspx***

**Б. Стандарди за заштита со лозинки**

Не користете иста лозинка за кориснички овластувања во Агенцијата за аудио и аудиовизуелни медиумски услуги како и за пристап кон други системи. Каде е можно, не користете иста лозинка за различни потреби, системи и апликации на Агенцијата за аудио и аудиовизуелни медиумски услуги.

Службените кориснички лозинките не се споделуваат со никој, освен со овластениот администратор во Секторот за информатички технологии. Сите лозинки треба да се третираат како осетлива, доверлива информација на Агенцијата за аудио и аудиовизуелни медиумски услуги. Корисниците на лозинките треба да се придржуваат кон следното:

- o Да не откриваат лозинка НИКОМУ.
- o Не се зборува за лозинката пред други.
- o Не се навестува форматот на лозинката (пр., "моето презиме").
- o Не се открива лозинката на прашаници или фомулари.
- o Не се разменува лозинка со членови на семејството.
- o Ако за време на отсуство има потреба од откривање на лозинката со друг корисник, тогаш по враќање на работа треба да се пристапи кон промена на лозинката.
- o Не користете "Remember Password" опција од апликациите .
- o Не ја запишувајте лозинката или чувате било каде во канцеларијата. Не ги чувајте лозинките на ниеден компјутерски систем и медиум без шифрирање.
- o Ако некој бара лозинка и добие пристап по дефинираната процедура, се упатува на овој документ.
- o Променете ја лозинката најмалку еднаш во три месеци.
- o Ако се сомнева дека корисничкото овластување или лозинката е компромитирано, пријави го инцидентот во Секторот за информатички технологии и модернизација и промени ги сите лозинки.

**Примена на стандардот**

Секој корисник на лозинки треба да се придржува кон Процедура за доделување и ракување со лозинки

**Прилог 2**

**Процедура за пристап и користење на Интернет**

### Вовед

Локалната компјутерска мрежа на Агенцијата за аудио и аудиовизуелни медиумски услуги дозволува пристап до ресурси и сервиси преку Интернет. Овој документ формално ја дефинира официјалната политика на Агенцијата за аудио и аудиовизуелни медиумски услуги во однос на користење на Интернет

### Намена

Агенцијата за аудио и аудиовизуелни медиумски услуги има либерален пристап на Интернет, но тоа не значи дека нема превенција на појавата на несоодветно, неетичко или незаконско однесување на сите корисници на информатичкиот компјутерски систем и телекомуникациската мрежа. Овие одговорности не само што се облигаторни по однос на деловниот интерес на Агенцијата за аудио и аудиовизуелни медиумски услуги, како и според законски и етички обврски кон доброто и приватноста на бизнис партнерите и корисниците на услугите – фирми и граѓаните.

### Обем

Обемот на оваа политика ги опфаќа следните информации:

- Интернет сервиси;
- Користење на ресурси;
- Очекувана приватност;
- Имиџ на Агенцијата за аудио и аудиовизуелни медиумски услуги ;
- Периодични ревизии.

Документот се фокусира на теми поврзани со серверите на Агенцијата за аудио и аудиовизуелни медиумски услуги, персонални сметачи, рутери, свичеви и други уреди кои поддржуваат пристап на Интернет.

Политиката за користење на Интернетот се однесува на сите корисници кои пристапуваат до Интернет, поединци кои работат во Агенцијата за аудио и аудиовизуелни медиумски услуги и кои имаат пристап до Интернет преку мрежните ресурси на Агенцијата за аудио и аудиовизуелни медиумски услуги. Од Интернет корисниците на Агенцијата за аудио и аудиовизуелни медиумски услуги се очекува да ги прифатат и да се придржуваат кон правилата од оваа политика. Исто така е потребно корисниците да го користат своето основно искуство и знаење за добро просудување додека ги користат интернет сервисите.

Пред да добие пристап до Интернет преку локалната мрежа, потенцијалниот Интернет треба да го прочита овој документ и потпише образец за прифаќање даден во прилог, кој треба да се потпише и достави до Секторот за информатичка поддршка и општи работи- Одделението за информатичка поддршка и технологии.

## 1. ЗАКАНИ ОД КОРИСТЕЊЕ НА ИНТЕРНЕТ

Неодговорното користење на Интернет може да претставува ризик за Агенцијата за аудио и аудиовизуелни медиумски услуги кон заштита на виталните информации сопственост на Агенцијата. Овие ризици вклучуваат:

**Несоодветно користење на ресурси**

Пристап до Интернет од страна на корисници кој не е неопходен за деловните потреби на Агенцијата за аудио и аудиовизуелни медиумски услуги може да резултира со злоупотреба на ресурсите. Овие активности може да делуваат на продуктивноста поради времето поминато во користење или "surfing" на Интернет.

**Лажна или погрешна информација**

Сите информации најдени на Интернет треба да се земат со резерва додека не се потврди нивната автентичност. На Интернет не постои контрола на квалитет, и голема количина на информации е неажурна или неточна.

## 2. ИНТЕРНЕТ СЕРВИСИ

Пристап на Интернет се дава на корисници за да се поддржат работните активности и единствено на основа на потребите за извршување на работите и професионални задачи.

**Кориснички сервиси**

Интернет пристап треба да се користи првенствено за деловни потреби. Можностите на стандардните Интернет сервиси ќе бидат на располагање на корисниците по потреба:

- ✓ E-mail – испраќање/примање E-mail пораки од/до Интернет преку локалниот маил сервер и локалната мрежа на градот (со или без документи во прилог, со одредени ограничувања во големината на пораката со прилозите). Се доделува на вработените во Агенцијата и членовите на Советот на Агенцијата.
- ✓ E-маил - проверка испраќање/примање E-mail пораки од/до Интернет преку web прелистувач од било која Интернет локација
- ✓ Навигација - WWW сервиси се неопходни за деловни потреби, користејќи HTTP алатка за сурфање.
- ✓ File Transfer Protocol (FTP) – испраќа и прима податоци, неопходни за деловни потреби, кои се во поголем обем.
- ✓ VPN пристап – виртуелна приватна конекција за контролиран безбеден пристап на вработените кога се надвор од Агенцијата или на службено патување до податоци сопственост на Агенцијата за аудио и аудиовизуелни медиумски услуги и други овластени лица за пристап до локалната мрежа и податоците за службени потреби.

Утврдена стратегија на Агенцијата е да се обезбеди Интернет навигација и службена е-маил адреса за секој негов службеник, вработен во Агенцијата за аудио и аудиовизуелни медиумски услуги , во локалната компјутерска мрежа.
Раководителите имаат право да додаваат и бришат сервиси според деловните потреби или промена на условите. Сите други сервиси ќе немаат авторизиран пристап од/кон Интернет и нема да бидат дозволени.

**Процедури за барање & одобрување**

Пристап до Интернет ќе се обезбеди за поддршка на деловни активности и само за потреби за вршење на работата на службениците. Пристап на Интернет за корисник му се дозволува по барањето од неговиот раководител.

## 3. КОРИСТЕЊЕ

**Користење на ресурси**

Пристап до Интернет ќе биде дозволен и обезбеден првенствено за деловни потреби. Интернет сервиси ќе се дадат на основа на тековните работни активности и одговорности на корисникот.

**Дозволено користење**

Користење на Интернет е доделен за поддршка на деловните активности неопходни за спроведување на работните задачи. Сите корисници мора да се придржуваат на принципите кои се однесуваат на користење на ресурсите и да применуваат добра проценка во користење на Интернет. Прашања мора да се упатуваат до Секторот за информатички технологии- Одделение за информатичка поддршка и технологии.
Користењето на Интернет за извршување на работните задачи може да вклучи:

- o Комуникација на вработените интерно и екстерно;
- o IT техничка поддршка за download на software и надградби ;
- o Преглед на web страни на вендори заради информации за продукти за набавка;
- o Пребарување на информации поврзани со извршување на работните задачи.
- o Истражување

**Користење за лични потреби**

Користење на компјутерските ресурси на Агенцијата за аудио и аудиовизуелни медиумски услуги за пристап на Интернет може да биде и за лични потреби, но само во време кога нема да пречи извршување на секојдневните обврски

Сите корисници на Интернет треба да се свесни дека на серверот на Агенцијата за аудио и аудиовизуелни медиумски услуги се создава историјат на користење на барањата за сервиси, внатрешни и надворешни адреси, кој периодично следи.

Корисници кои ќе одберат да чуваат или испраќаат лични податоци (кредитни картици, состојба на сметки, и слично), го прават тоа на свој ризик. Агенцијата за аудио и аудиовизуелни медиумски услуги не е одговорна за губење на тие информации

**Забрането користење**

- Не е дозволено собирање, чување и разнесување на податоци кои се нелегални, порнографски или кои промовираат расна, национална, полова или верска нетрпеливост во и од мрежата на Агенцијата.
- Агенцијата за аудио и аудиовизуелни медиумски услуги исто така не дозволува водење на фирма, политичка активност, вклучување во измами, или свесно ширење на погрешни информации.
- Пристап до информации на Агенцијата за аудио и аудиовизуелни медиумски услуги кои не се согласно работата на корисникот Овде се вклучува неавторизирано читање на информациите за кориснички овластувања, неавторизиран пристап до персоналната евиденција, и информации кои не се потребни за извршување на работните задачи.
- Користење, пренос, копирање на материјали со што се прекршуваат правата на сопственост на податоци на лица или фирма.
- Пренос на лични, доверливи или сензитивни информации без соодветна контрола.
- Неавторизирано симнување (download) на било какви привремени (shareware) програми или електронски запис за користење без авторизација.
- Играње игри, игри на среќа, online обложување, итн.
- Препраќање на писма во ланец.
- Учество на интерактивен натпревар.
- Прифаќање на промоциски податоци.
- P2P апликации (Torrent download)

Опсегот на интерната мрежа како и врската со Интернет се дели од сите корисници на Агенцијата за аудио и аудиовизуелни медиумски услуги, и се ограничени ресурси. Корисниците треба да направата разумен напор да го користат овој ресурс на начин кој не делува негативно на другите вработени.

**Software Лиценци**

Репродукција на материјали со пристап преку Интернет мора да се направи само со дозвола на авторот или сопственикот на документот.

**Очекувања за приватност**

**Мониторинг**

Интернет активностите периодично се следат и може да се ограничат по потреба.
Бидејќи сите ИКТС и документите кои се продуцираат од нив се сопственост на Агенцијата за аудио и аудиовизуелни медиумски услуги, Директорот / заменик на директорот на Агенцијата можат со писмен налог до раководителот на Секторот за информатичка поддршка и општи работи да наложат проверка на

службениот e-mail, службените фолдери, web пристапот, и други информации кои се чуваат на компјутерите на Агенцијата за аудио и аудиовизуелни медиумски услуги во било кое време и без најава.

**E-mail тајност**

За Директорот/заменик на директорот на Агенцијата како и раководителите на секторите се препорачува примената на дигиталните сертификати во заштита на електронската пошта со што се гарантира доверливоста на пораката, идентитетот на авторот и содржината.

Платформата за електронската пошта на Агенцијата за аудио и аудиовизуелни медиумски услуги е Outlook Express/ Microsoft Outlook , кој претставува POP3 протокол, кој пристигнатите пораки ги симнува (download-ира) локално, со што одговорноста за истите ја носи самиот корисник. Платформата на Агенцијата поддржува интерфејси кои се во согласност со SMTP/MIME стандард како внатрешна безбедност за да се осигура доверливост на E-поштата, а за надворешна комуникација користи стандард за безбедна размена на пораки - S/MIME-V3. Некои од сигурносните можности на е-маил платформата (Outlook Express , Microsoft Outlook) кои се користат се : пристап до поштенските сандачиња само на сопствениците (и администраторот) со лозинка, можност сами да ја менуваме лозинката, различна или иста лозинка со Windows лозинката или со Web/Интернет лозинката, пристап преку интернет пребарувач итн.

**Заштита на податоци и информации**

Податоците и информациите во електронска форма кои се означени како заштитени треба да се управуваат и пренесуваат во согласност со одредбите на систем за управување со информатичка безбедност. Податоците кои не се означени како заштитени треба да се управуваат и пренесуваат во согласност со рамката на безбедност на информации за јавните сервиси.

Податоците достапни преку е-сервисите на Агенцијата за аудио и аудиовизуелни медиумски услуги треба да бидат така дизајнирани за да обезбедат заштита од безбедносни ризици при поврзување и пренос преку интернет, вклучувајќи ја и можноста за заштита од симнување на содржини

По исклучок податоците и информациите ќе се доставуваат во по електронска пошта или на електронски медиум. При достава со електронска пошта препорачливо е електронско потпишување и енкрипција на податоците со електронски сертификат од овластен издавач на сертификати. При размена на електронски медиум размената се врши преку овластени лица за предавање и примање на податоците, за што ќе се води уредна евиденција.

**Заштита на лични податоци**

Приватноста и заштитата на личните податоци на физичките лица се дел од безбедносниот систем на Агенцијата за аудио и аудиовизуелни медиумски услуги. Корисникот на информациските и комуникациските услуги, е-сервиси кои ги дава Агенцијата за аудио и аудиовизуелни медиумски услуги , треба да е целосно заштитен од злоупотреба на неговите лични податоци и неговата приватност. Ова подразбира дека Агенцијата за аудио и аудиовизуелни медиумски услуги треба да ги преземе сите технички и организациони мерки за да ја заштити приватноста на корисниците согласно со постојните законски прописи во државата.

**Одржување на имиџот на Агенцијата за аудио и аудиовизуелни медиумски услуги**

- ✓ Кога се користат ресурсите на Агенцијата за аудио и аудиовизуелни медиумски услуги за пристап и користење на Интернет, корисниците мора да прифатат дека ја претставуваат Агенцијата за аудио и аудиовизуелни медиумски услуги .
- ✓ Периодично ќе се тестира степенот на примената на политиката на користење на Интернет

**Прилог 3**

**Процедура за ракување и чување на ИТ опрема**

**Цели**

- Да се обезбеди ефикасен систем за евидентирање и чување на информатичка опрема и ИТ проекти
- Да се дефинираат неопходни активности и мерки со кои се обезбедува квалитетно ракување со опремата

**Глобален опис на Процедурата**

Процедурата се однесува на ракување, односно користење и чување на:

- информатичка опрема која е составен дел на секое работно место - хардвер, софтвер - работна станица, со која се задолжува секој **вработен лично и одговара** за нејзино чување и користење
- мрежна и комуникациска опрема и системски софтвер, задолжен е Секторот за информатичка поддршка и општи работи- Одделение за информатичка поддршка и технологии .
- апликативни решенија инсталирани на мрежата, за кои од аспект на содржина се задолжени корисниците, а од аспект на функционалност е задолжен Секторот за информатичка поддршка и општи работи
- backup и чување на копии на податоци

Со оваа процедура се дефинираат правилата и задолженијата кои мора да ги исполнуваат сите корисници на опремата, правилата за работа во мрежа, заштита од вируси и back-up на податоци.

**Дефиниции во процедурата**

- информатичка опрема: хардвер, софтвер и комуникациска опрема
- работна станица: персонален компјутер со основна конфигурација (процесор, монитор, тастатура) и дополнителна опрема - принтери, сканери,мултимедиа, ...
- мрежна и комуникациска опрема: сервери, мрежни уреди (HUB, SWITCH), мрежна инсталација, комуникациски уреди (Router, Modem) и системски и мрежен софтвер
- апликативни решенија - проекти кои се инсталирани на мрежа, наменети за заедничко користење
- корисници на опрема - сите вработени кои користат информатичка опрема
- Back up копија на мрежните дискови во функција на осигурување со последна верзија на активните апликации, бази на податоци, бази на документи во Интранетот, бази на електронската пошта, копија на системски диск од серверите со disaster recovery, копија од Интернет/Интранет апликации и друг SW во случај на непредвидени оштетувања

## АКТИВНОСТИ И ОДГОВОРНИ ЛИЦА

| Активност | Одговорен |
|---|---|
| • Евидентирање на информатичка опрема и задолжувања<br>• Обезбедување на квалитетно функционирање на локална компјутерска мрежа и нејзино одржување<br>• Сигурност и заштита на опрема и содржините во системската сала. Интервенција на надворешно лице во систем сала задолжително претходно се најавува и не е дозволено негово присуство без придружба од овластено лице од секторот<br>• Заштита од вируси преку имплементирање на безбедносни политики<br>• back up копија на апликации, бази на податоци, бази на документи, електронска пошта и системски записи на сервер и работни станици<br>• водење евиденција на лиценциран SW<br>• водење на база на податоци на опрема<br>• водење шематски приказ на компјутерска мрежа | Помлад референт/ Соработник / виш соработник |
| • Користење информатичка опрема и проекти во локална мрежа, согласно добиеното Задолжение за опрема и Правилата за работа во мрежа | Интерен корисник |
| • Business Continuity План | Раководител на СИПОР |
| • Пропишува Информатички Безбедносни политики, процедури, прирачници и водичи | Раководител на СИПОР |

## РАКУВАЊЕ И ЧУВАЊЕ НА КОМПЈУТЕРСКА ОПРЕМА

**Ракување и чување на компјутерска опрема ги опфаќа персоналниот компјутер, дополнителната опрема и системски софтвер инсталиран на работната станица, со која се задолжува секој вработен лично и одговара за нејзино чување и користење**

| Активност | Одговорност |
|---|---|
| Со набавка на ИКТС опрема, врши прием и евидентирање во Базата на опрема, со што секој елемент се класифицира и еднозначно се нумерира. | Соработник / виш соработник/ Магационер |
| Доставува писмено известување за распоредување на опрема со назначување на локација и лице које со опремата ќе работи. | Раководител на СИПОР, интерен корисник |
| Доставува писмено известување за нови вработувања и распоредувања на вработените | Сектор за правни работи |
| Подготвува Листа за задолжение кои се чуваат во регистратор, до промена на задолжување. При раздолжување подготвува Листа за раздолжување | Раководител на СИПОР |
| Листата за задолжување се потпишува од страна на корисникот, со што станува одговорен за физичко чување на опремата, начинот на користење на работната станица и почитување на правилата за работа во мрежа. | Интерен корисник |

## РАКУВАЊЕ И ЧУВАЊЕ НА МРЕЖНА И КОМУНИКАЦИСКА ОПРЕМА

Ракување и чување на мрежна и комуникациска опрема опфаќа сервери, мрежни уреди, мрежна инсталација, комуникациски уреди, системски и мрежен софтвер

| Активност | Одговорност |
|---|---|
| • Врши задолжување на вишиот соработник со инсталирана мрежна и комуникациска опрема | Раководител на СИПОР/ ОИПТ |
| • Ја прима и евидентира инсталираната опрема во базата на опрема<br>• Ја евидентира во шематскиот приказ на компјутерската опрема<br>• Организира инсталирање, сместување и чување на мрежната и комуникациска опрема<br>• Ја документира мрежната инфраструктура и соодветната опрема. Документацијата се чува во просториите на СИПОР<br>• Врши континуиран надзор на функционирањето на мрежата и комуникациите и организира одржување.<br>• Организира заштита на мрежата од вируси и обезбедува ажурност на антивирус програмите | Раководител / Виш соработник |
| • Ги одобрува и пропишува Правилата за работа во мрежа и ИТ безбедносна политика | Раководител |

## РАКУВАЊЕ И ЧУВАЊЕ НА АПЛИКАТИВНИ РЕШЕНИЈА

Ракување и чување на апликативни решенија ги опфаќа проектите кои се инсталирани на мрежа, наменети за заедничко користење и започнува во моментот на примопредавање на апликативно решение во редовна експлоатација

| Активност | Одговорност |
|---|---|
| • Ја организира инсталацијата и надградбата на новите верзии на апликативните решенија на серверите во систем салата. Во случај на потреба од инсталација на серверските машини од надворешен консултанти/проектанти, најава за интервенција и работа во систем сала дава службата чија апликација се надградува, еден ден претходно, во договор со систем инженерот.<br>• Организира и врши редовно земање на back up копии од мрежните дискови<br>• Back up Копија се зема дневно, неделно, квартално, еднаш годишно или периодично почесто, по специјално барање на корисникот одговорен за одржување на апликативното решение<br>• Се чува тековна состојба на податоци наназад три месеца, кварталните копии се чуваат 12 месеци и годишните 5 години пред да бидат прекриени. | Соработник / Виш соработник |
| • Одговара за начинот на користење на апликативното решение и точноста на податоците.<br>• Корисникот ја дефинира специјалната потреба од земање на копии од податоци и го дефинира интервалот на чување на копиите. | Интерен корисник |

## BACK UP И ЧУВАЊЕ НА КОПИИ НА ПОДАТОЦИ

Back up и чување на копии на податоци опфаќа постапка за правење на back up, динамика на земање на копија, локација на чување на копии на податоци од апликативни решенија на проекти кој се инсталирани на мрежа. Back up копија на мрежните дискови во функција на осигурување со последна верзија на активните апликации, бази на податоци, бази на документи во Интранетот, бази на електронската пошта.

| Активност | Одговорност |
|---|---|
| • Снимените материјали од радиодифузерите во зависност од покриеноста се чуваат 120 и 90 дена во централниот сториџ на Агенцијата.<br>• Копија од податоците на серверите се зема на диск на file серверот или сториџот еднаш дневно и на друг сервер за back up, еднаш дневно/неделно.<br>• Верзии на документите на File серверот се чуваат со функцијата shadow copy.<br>• Копиите земени по специјално барање на службите се чуваат во период одреден од службата.<br>• Годишните копии се чуваат до 5 години наназад.<br>• Процедурата за back up отпочнува попладне во 20 часот, по истек на работното време. За податоци од посебна важност се прават и годишни, полугодишни или периодични копии на трака, ДВД/ЦД, трака или друг медиум, на барање на одговорната служба<br>• Едната копија заедно со прегледот се чува во метален ормар во систем салата во СИПОР .<br>• Периодично да се прави проверка на направениот backup | Соработник / Виш соработник |

***ПЛАН ЗА BACK-UP***

Backup се прави според претходно утврдена динамика и процедура дефинирана во следната табела.

| Машина | Апликација | Форма | Динамика | Локација |
|---|---|---|---|---|
| SQL server<br>192.168.1.31 | НАВС<br>Кабелски оператори<br>Кадровски менаџмент | HDD<br>DVD<br>Екстерен HDD | Дневно<br>Неделно<br>Годишно<br>Годишно | АГЕНЦИЈА<br>Сеф (надвор)<br>АГЕНЦИЈА / Сеф<br>АГЕНЦИЈА |
| File server<br>192.168.1.51 | Документи за споделување (Заеднички документи) | HDD | Дневно | АГЕНЦИЈА |
| Сервери DC<br>192.168.1.26 | Копија од Active Directory | HDD | Месечно | АГЕНЦИЈА |
| Сите Сервери | Копија од системски file-ови, OS | HDD | Квартално<br>Годишно | АГЕНЦИЈА/СЕФ |
| Виртуелна машина<br>192.168.1.24 | Интегриран софтвер за архивско, финансиско и економско работење | Виртуелен Диск, и HDD | Неделно<br>Годишно | АГЕНЦИЈА/СЕФ |

**Прилог 4**

**ИТ безбедносна политика – Образец за прифаќање**

По читањето на документот – Безбедносна политика, Ве молиме да го потпишете овој образец и да го доставете до Секторот за информатичка поддршка и општи работи за ИКТ технологија.

Со потписот даден подолу, вработениот кој добива пристап до сервисите преку ресурсите на локалната компјутерска мрежа на Агенцијата за аудио и аудиовизуелни медиумски услуги, е информиран, прифаќа и се согласува со ИКТ безбедносната политика. Потписот исто така потврдува дека тој/таа го прочитал и разбрал текстот на оваа политика пред да се потпише овој образец.

Нема да се дозволи пристап до ресурсите на локалната компјутерска мрежа, се додека овој образец не се потпише. По комплетирањето на образецот, податоците се внесуваат во базата за човечки ресурси и во база специјално водена за евидентирање на правата за пристап во Сектор за информатичка поддршка и општи работи и модернизација. Овој образец е предмет на интерна проценка.

**СОГЛАСНОСТ**

**Потврдувам дека ја прочитав ИКТ безбедносната политика. Ја разбрав содржината и се согласувам да го почитувам кажаното во Политиката.**

**Сектор/Одделение** _____

**Деловна функција** _____

**Име** _____

**Потпис** _____

**Датум** _____/_____/_____ **година**

**Совет на Агенцијата за аудио и аудиовизуелни медиумски услуги,**
**Претседател на Советот**

_____
**Лазо Петрушевски**

Бр. 01-2801/1
16.06. 2017 година
Скопје