Врз основа на член 23 од Законот за заштита на личните податоци (Службен весник на РМ 7/05,103/08 и 124/10) и одредбите од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработка на личните податоци („Сл. весник на РМ“ бр. 38/09), а в.в. со Одлуката за измени и дополнувања на Правилникот за технички и организационите мерки за тајност и заштита на личните податоци бр. _____ Сенатот на Универзитетот Американ Колеџ Скопје на ден 03.07.2013 донесе

ПРАВИЛНИК

за техничките и организациските мерки за обезбедување тајност и заштита на личните податоци

(пречистен текст)[1]

1. Општи одредби

Предмет на уредување

Член 1

Со овој Правилник се пропишуваат техничките и организационите мерки за обезбедување тајност и заштита на обработката на личните податоци што ги применува Универзитетот Американ Колеџ Скопје – Скопје (во натамошниот текст: Универзитет).

2. Поимник

Член 2

1. *Администратор на информацискиот сис*тем е лице овластено за планирање и за применување на технички и организациони мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци.

2. Личен податок е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува врз основа на матичен број на граѓанинот или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, ментален, економски, социјален или културен идентитет.

3. Збирка на лични податоци е структурирана група лични податоци која е достапна согласно специфични критериуми.

4. Контролор на збирка на лични податоци е физичко или правно лице, кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци.

[1] Одредбите и поимите кои во пречистениот текст во закосена форма, се донесуваат на Правилникот за изменување и дополнување на Правилникот за техничките и организационите мерки за обезбедување тајност и заштита на обработката на личните податоци(Службен весник на РМ бр. 158/10).

5. *Овластено лице* е лице вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и до информатичко комуникационата опрема.

6. Медиум е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на кој податоците можат да бидат снимени или од кој истите можат да бидат повторно вратени.

7. Обработувач на збирки на лични податоци е физичко или правно лице или законски овластен државен орган кој ги обработува личните податоци за сметка на Контролорот.

8. *Офицер за заштита на лични податоци е лице овластено од контролорот за самостојно и независно вршење на работите во смисла на член 26-а од Законот за заштита на личните податоци.*

9. Сигурносна копија е копија на личните податоци содржани во електронските документи кои се зачувани на медиум за да се овозможи нивно повторно враќање.
8. Субјект на лични податоци е секое физичко лице на кое се однесуваат обработените податоци.

3. Збирки на податоци

Член 3

Универзитетот како Контролор на лични податоци, води збирки на лични податоци.

Збирките од став (1) од овој член се евидентираат во посебен лист „Евиденција за збирки на лични податоци и централен регистар“, кој е составен дел на овој Правилник (Прилог 2).

Документација за збирките од став (1) од овој член се води во посебни досиеја и се чува во огноотпорни метални фиоки, во просториите (архиви) на Службата на студентски прашања и службата за човекови ресурси. Просториите се под видео надзор.

Правото на пристап до архивите на досиеја се пропишува со акти на Универзитетот.

4. Обработка на личните податоци

Член 4

Одредбите од овој Правилник се применуваат за :

- целосно и делумно автоматизирана обработка на лични податоци

- друга *рачна* обработка на лични податоци што се дел од постојаната збирка на лични податоци или се наменети да бидат дел од збирката на лични податоци.

Обработката од став (1) од овој член се врши во работните простории на Универзитетот.

Обработка на податоци надвор од работните простории на Универзитетот, се врши врз основа на писмено овластување од страна на Универзитетот и во согласност со соодветното ниво на техничките и организационите мерки кои се применуваат за обработка на податоците.

Член 4 а

Универзитетот, како контролор на лични податоци, може да пренесе работи од неговиот делокруг на работа поврзани со обработката на лични податоци на обработувач на лични податоци.

Меѓусебните права и обврски помеѓу контролорот и обработувачот се уредуваат со договор во писмена форма, кој содржи обврска обработувачот на лични податоци да постапува единствено во согласност со добиените упатства од контролорот и да преземе технички и организациски мерки за да обезбеди тајност и заштита на обработката на личните податоци.

Член 5

Во рамките на Универзитетот се врши и обработка на лични податоци преку вршење на видео надзор .

Видео надзор се врши во архивите во кои се чуваат досиејата на студентите и вработените, како и архивите во кои се чува целокупната испитна документација.

Универзитетот врши видео надзор и заради заштита на својата сопственост.
За вршењето на видео надзор во деловните простории, навремено се известуваат сите вработени и студентите.

На местата каде се врши видео надзор истакнато е известување.

Известувањето од став 4 од овој член ги содржи следните информации :
- дека се врши видео надзор
- кој го врши надзорот
- за начинот на кој може да се добијат информации за тоа каде и колку време се чуваат снимките од системот за видео надзор.

Снимките направени при вршење на видео надзор се чуваат до исполнување на целите за кои се врши, а најмногу 30 дена од денот на кој е извршен видео надзорот.

5. Нивоа на технички и организациони мерки

Член 6

Техничките и организационите мерки од член (1) од овој Правилник, се класифицираат во две нивоа:

- основно
- средно

За сите документи задолжително се применуваат технички и организациони мерки кои се класифицирани на основно ниво.

За документи кои содржат лични податоци што се однесуваат на изречени казни и мерки за извршени прекршоци, се применуваат технички и организациони мерки кои се класифицирани на основно и средно ниво.

За документите кои содржат матичен број на субјектот, се применуваат технички и организациони мерки кои се класифицирани на основно и средно ниво.

Универзитетот како Контролор на лични податоци води сметка матичниот број на субјектот да не биде непотребно видлив, печатен или превземен од збирката на лични податоци.

6.Технички мерки

Член 7

Техничките мерки кои ги превзема Универзитетот во поглед на тајност и заштита на личните податоци се следните :

1. Определување единствено корисничко име кое овозможува пристап на *овластено лице* до поединечни апликации или до информатичкиот систем во целина
2. Определување лозинка креирана за *секое овластено лице* која содржи која содржи: карактери,бројки и симболи. Лозинката е составено од минимум 8 алфа- нумерички знаци (од кои минимум една голема буква) и специјални знаци и истата се менува секои 3 месеци.
3. Определување јасна идентификација на *секое овластено лице* кое пристапило до информацискиот систем.
4. Проверка на авторизацијата на *секое овластено лице*.
5. Автоматизирано одјавување од информатичкиот систем после изминување на 15 минути неактивност.
6. Инсталирана хардверска/софтверска заштитна мрежна бариера (firewall) и рутер помеѓу информацискиот систем и интернет, како заштита од недозволени или злонамерни обиди за влез или пробивање на системот.
7. Ефективна и сигурна анти-вирусна и анти – спам заштита , која постојано се ажурира.

7.Организациони мерки

Член 8

Организациони мерки кои ги презема Универзитетот во поглед тајност и заштита на личните податоци се следните:

1. Ограничен пристап или идентификација на пристап до личните податоци.
2. Обезбедување физичка сигурност на работните простории и на информатичко комуникациската опрема каде се собираат, обработуваат и чуваат личните податоци .
3. Обезбедување физичка сигурност на информацискиот систем со тоа што просторијата во која се наоѓа серверот т.е. софтверските програми за обработка на личните податоци се физички одвоени во посебна просторија во која пристап имаат лица – администратори овластени од Универзитетот.
4. Сите лица кои се вработуваат или се ангажираат од страна на Универзитетот, пред нивното започнување со работа се запознаваат со прописите за заштита на личните податоци. Истовремено при стапување во работен однос или при нивно ангажирање, тие потпишуваат изјава за тајност и заштита на обработката на личните податоци, која е составен дел на овој Правилник (Прилог 1)
5. Контролорот води евиденција на лица овластени да вршат обработка на лични податоци, која е составен дел на овој Правилник (Прилог 3).
6. *Контролорот задолжително врши континуирано информирање на овластените лица за непосредните обврски и одговорности за заштита на личните податоци“*

8. Одговорно лице и комисија за заштита на личните податоци

Член 9

Универзитетот овластува лице за заштита на личните податоци.

Лицето од став еден од овој член е одговорно за координација и контрола на постапките и упатствата утврдени во документацијата за техничките и организационите мерки.

Универзитетот формира и комисија за заштита на личните податоци која ќе го надгледува спроведувањето на пропишаните организациони и технички мерки за заштита на личните податоци .

Комисијата од став (3) од овој член расправа по поднесена пријава за сторени дејствија на повреда на тајноста и заштитата на личните податоци и спроведува соодветни дисциплински мерки.

9. Правила за определување на обврските и одговорностите на *овластените лица и администраторот на информацискиот систем* при користење на документите и информатичко комуникациската опрема

9.1. Обврски и одговорности на *овластените лица*

Член 10

Овластеното лице е должно да се запознае и да дејствува согласно техничките и организационите мерки околу заштита на личните податоци.

На секое овластено лице, *администраторот на информацискиот систем* му доделува единствено корисничко име и лозинка за пристап до одредени апликации на информацискиот систем. Не е дозволливо и е казниво користење на туѓо корисничко име и лозинка.

Доколку овластеното лице има потреба од пристап до дополнителни апликации на информацискиот систем, го известува неговиот непосредно надреден, кој доколку ја оправда потребата од дополнителен пристап до информацискиот систем, поднесува писмено барање *до администраторот на информацискиот систем .*

Доколку се евидентира дејствие кое влијае врз нарушување на тајноста и заштитата на личните податоци, се пријавува до комисијата за заштита на личните податоци.

9.2. Обврски и одговорности на *администраторот на информацискиот систем*

Член 11

Администраторот на информацискиот систем е целосно запознат со актите за техничките и организационите мерки околу заштита на личните податоци како и со последиците од дејствијата кои влијаат врз нарушувања на тајноста на личните податоци.

Универзитетот го *овластува администраторот на информацискиот систем* од став еден од овој член со целосен авторизиран пристап до сите лични податоци / збирки на податоци со кои располага Универзитетот.

Администраторот на информацискиот систем води евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем и воспоставува постапки за идентификација и проверка на авторизиран пристап. Информацискиот системот е прилагоден автоматски да врши проверка и авторизација во доменот - дата база на овластени лица .

Во евиденцијата од став (3) од овој член се внесуваат и нивоата на авторизиран пристап на секое овластено лице.

Администраторот на информацискиот систем може да доделува, менува и одзема авторизиран пристап до личните податоци и информатичко комуникационата опрема на овластени лица .

Член 11 –а

Обврските и одговорностите на администраторот на информацискиот систем , контролорот ги дефинира и утврдува во Правилата за определување

на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема.

Контролорот задолжително врши периодична контрола на работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.
Во извештајот од ставот (2) од овој член треба да се содржани констатираните неправилности и предложените мерки за отстранување на тие неправилности.

10. Правила за начинот на правење сигурносна копија, архивирање и чување, како и за повторно враќање на зачувани лични податоци

Член 12

Сигурносните копии задолжително се прават секој работен ден и на крајот на работната седмица, а по потреба и секој последен ден во месецот.

Сигурносните копии од став (1) од овој член се чуваат надвор од објектот во кој е сместен информацискиот систем на универзитетот.

Пристап до сигурносните копии имаат само овластени : администратори и лице одговорно за заштита на лични податоци. Овие лица се овластени од Универзитетот за координирање и контрола на техничките и организационите мерки кои се применуваат за тајност и заштита на личните податоци.

Сигурносните копии од став (1) од овој член се физички и криптографски заштитени (снимени се на ДВД медиум кој не може да се едитира – write once), заради оневозможување на било каква модификација.

Сигурносните копии задолжително се прават на начин со кој ќе се гарантира постојна можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

Контролорот задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци согласно ставот (5) од овој член.

Сигурносните копии се чуваат надвор од серверите и треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

11. Правила за начинот на уништување на документите, уништување, бришење и чистење на медиумите

Член 13

Универзитетот ги користи следните видови на медиуми: CD, DVD и HDD.

По пренесување на личните податоци на медиумот, тој се чува во банкарски сеф.
Во службата за ИТ се врши евиденција на секој примен медиум како и на медиумите кои се искористени за снимање на лични податоци. Евиденцијата содржи и податок за типот на личните податоци содржани на медиумот.

Уништување на медиумот се врши со механичко разделување на неговите составни делови, при што тој станува неупотреблив. Бришење или чистење на медиум се прави на тој начин со што се оневозможува понатамошно обновување на снимените лични податоци.

При уништувањето, бришењето или чистењето на медиумот се составува записник кој содржи податоци за целосна идентификација на медиумот како и категории на лични податоци снимени на него.

При пренесување на медиумот надвор од просториите на Универзитетот, се применуваат сите мерки за заштита при транспорт на медиуми со цел да се спречи неовластено обработување на личните податоци снимени на нив.

12. Друга рачна обработка на личните податоци
12.1 Основно ниво на технички и организациони мерки

Член 14

Одредбите од членовите 4 ,6,8 и 10 соодветно се применуваат и при друга рачна обработка на личните податоци што се дел од постојната ,збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

12.1.1 Пристап до документите

Член 15

Пристапот до документите треба да биде ограничен само за овластени лица на контролорот.
За пристапување до документите задолжително треба да се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.
Доколку е потребен пристап на друго лице до документите тогаш треба да бидат воспоставени соодветни процедури за таа цел во документацијата за техничките и организационите мерки.

12.1.2. Правило на „чисто биро“

Член 16

Контролорот задолжително го применува правилото „чисто биро“ при обработка на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

12.1.3 Чување на документите

Член 17

Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.
Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот 1 од овој член, контролорот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.
Ако документите . не се чуваат заштитени на начин определен во ставовите 1 и 2 од овој член, тогаш контролорот треба да ги примени ситре мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

12.1.4 Уништување на документи

Член 18

Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно да не можат да бидат употребливи.
Во случајот од ставот 1 на овој член комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на лични податоци содржани во истиот.

12.2. Средно ниво на технички и организациони мерки

12.2.1 Контрола

Член 19

Одредбите од членот 6 соодветно се применуваат и при друга рачна обработка на личните податоци што се дел од постојаната збирка на лични податоци или се наменети да бидат дел на збирката на лични податоци.

12.2.2 Контрола на информацискиот систем и информатичката инфраструктура

Член 20

Информацискиот систем и информатичката инфраструктура на УАКС задолжително подлежат на внатрешна и надворешна контрола со цел да се провери дали постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци.

УАКС врши надворешна контрола на информацискиот систем и информатичката инфраструктура на секои три години, а внатрешна контрола секоја година.

Надворешната контрола од став (1) на овој член се врши преку обработка на документи од страна на независно трето *правно* лице.

Во извештајот од извршената контрола од ставот (1) на овој член задолжително треба да има мислење за тоа во колкава мера постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци, да се наведени констатираните недостатоци, како и предложените неопходни корективни или дополнителни мерки за нивно отстранување.

Во извештајот од ставот (4) на овој член треба да се содржани и податоците и фактите врз основа на кои е изготвено мислењето и се предложени мерките за отстранување на констатираните недостатоци.

Извештајот од ставот (4) на овој член се анализира од страна на *офицерот* за заштита на личните податоци, кој доставува предлози на контролорот за преземање на потребните корективни или дополнителни мерки, за отстранување на констатираните недостатоци.

Извештајот од ставот (4) на овој член треба да биде достапен за увид на Дирекцијата за заштита на личните податоци.

Образецот на извештајот од ставот (4) на овој член е составен дел (Прилог 4)

12.2.2 Евидентирање на авторизираниот пристап (логови)

Член 21

УАКС води евиденција за секој авторизиран пристап која треба да ги содржи особено следните податоци: име и презиме на овластеното лице, работна станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

Во евиденцијата од ставот (1) на овој член се внесуваат и податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.

Операциите кои овозможуваат евидентирање на податоците од ставовите (1) и (2) на овој член треба да бидат контролирани од страна на *офицерот* за заштита на личните податоци и истите не може да се деактивираат.

Евиденцијата од ставот (1) на овој член се чува најмалку *пет* години.

Офицерот за заштита на личните податоци врши периодична проверка на податоците од ставовите (1) и (2) на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

12.2.3 Начин на чување на документите

Член 22

Плакарите (орманите) , картотеките или другата опрема за чување на документи задолжително треба да бидат сместени во простории заклучени со соодветни заштитни механизми. Просториите треба да бидат заклучени и за периодот кога документите не се обработуваат од овластените лица.
Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (1) од овој член, контролорот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

12.3. Високо ниво на технички и организациски мерки
12.3.1 Копирање или умножување на документите

Член 23

Копирањето или умножувањето на документите може да се врши единствено со контрола на овластени лица определени со претходно писмено овластување од страна на контролорот.

Уништувањето на копиите или умножените документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

12.3.2 Пренесување на документи

Член 24

Во случај на физички пренос на документите контролорот задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои се пренесуваат

13. Завршни одредби

Член 25

Одредбите од овој Правилник се применуваат на сите организациони единици во рамките на Универзитетот.

Член 26

Овој Правилник влегува во сила со денот на донесувањето. Со донесувањето на овој Правилник престанува да важи Правилникот за техничките и организационите мерки за тајност и заштита на личните податоци бр. 07 – 33/7 од 24.01.2011 година.

Универзитетски Сенат

Ректор

Проф. д-р Марјан Бојаџиев

_____

И З Ј А В А

Јас, _____, под полна морална и материјална одговорност изјавувам дека ќе ги почитувам начелата за заштита на личните податоци при пристапот до нив и дека нивната обработка ќе ја вршам согласно Правилникот на Универзитетот за техничките и организационите мерки за обезбедување тајност и заштита на обработка на личните податоци, ќе ги третирам како доверливи и ќе преземам мерки за нивна заштита.

Датум _____ Изјавил,

_____