Телефон: +38946511000
Факс: +38946511567
www.uist.edu.mk

Партизанска бб.
6000 Охрид
Република Северна Македонија

Бр. 01-83/1
Охрид, 27.1.2022 год.

Врз основа член 94 од Законот за високото образование („Службен весник на Република Македонија” бр. 82/2018 и 197/2021) во врска со член 6 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија” бр 122/20), Сенатот на Универзитетот за информатички науки и технологии „Св. Апостол Павле” Охрид, на седницата одржана на ден 27.01.2022 донесе

ПРАВИЛНИК
За безбедност при обработка на личните податоци во Универзитетот за информатички науки и технологии ,,Свети Апостол Павле” Охрид

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој Правилник се пропишуваат техничките и организациските мерки за информацискиот систем и информатичката структура при обработка на личните податоци во Универзитетот за информатички науки и технологии „Свети Апостол Павле“ Охрид, (во натамошниот текст: Универзитетот).

Член 2

Одредбите од овој Правилник се применуваат за:
– целосно и делумно автоматизирана обработка на личните податоци;
– друга рачна обработка на личните податоци што се дел од постојната збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Член 3

Земајќи ги предвид природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица, Универзитетот како контролор е должен да примени соодветно ниво на технички и организациски мерки кое ќе биде пропорционално и на активностите за обработка на личните податоци

Техничките и организацизациските мерки од точка 1 на овој член се класифицираат во две нивоа:

- стандардно ниво и
- високо ниво.

Член 4

Универзитетот е одговорен за усогласеноста во однос на нивото на мерки за безбедност на обработката на личните податоци кое ќе го примени во согласност со член 3 од овој Правилник, при што треба да обезбеди соодветно ниво на безбедност на личните податоци, вклучувајки заштита од неовластена или незаконска обработка како и заштитата од нивно случајно губење, уништување или оштетување.

Универзитетот ја демонстрира примената на мерките според барањата утврдени во ставот 1 на овој член вклучувајки ги причините и основите за изборот на примената на стандардното, односно високото ниво.

Член 5

За сите документи задолжително ќе се применуваат технички и организациски мерки класифицирани на стандардно ниво.

За документите кои содржат матичен број на граѓанинот задолжително се применуваат техничките и организациските мерки кои се класифицираат на стандардно ниво.

За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на лични податоци и/или матичен број на граѓанинот, задолжително се применуваат технички и организациски мерки кои се класифицирани на стандардно и високо ниво.

II. ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 6

Универзитетот врши евидентирање и ја чува целокупната документација за софтверските програми за обработка на личните податоци и сите негови промени.

Член 7

Вработените во ИТ центарот во Универзитетот се должни да вршат одржување на информатичкиот систем во Универзитетот, согласно со документацијата за техничките и организациските мерки.

III. СТАНДАРДНО НИВО

Документација за технички и организациски мерки на стандардно ниво

Член 8

Универзитетот во Политиката за системот за заштита на личните податоци ги утврдува и начелата за безбедност и заштита на личните податоци.

Врз основа на Политиката за системот за заштитата на личните податоци, Универзитетот донесува подетални политики и процедури во кои се опишанио техничките и организациските мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичка инфраструктура.

Документацијата од ставот (2) Универзитетот ја менува и дополнува кога ќе се направат промени во информацискиот систем и информатичката инфраструктура, а најмалку еднаш годишно врши нејзино оценување, евалуација и ажурирање.

Технички мерки

Член 9

Во Универзитетот се обезбедуваат следниве технички мерки за тајност и заштита при обработката на личните податоци:

1. Единствено корисничко име за секој вработен;

2. Лозинка креирана за секој вработен посебно, составена од комбинација на најмалку8 (осум) алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;
3. Автоматизирано одјавување од информатичкиот систем по изминување на определен период на неактивност (не подолго од 15 минути) и за повторно активирање на системот епотребно повторно внесување на лозинка;
4. Автоматизирано блокирање на Информацискиот систем по три неуспешни обиди (внесување на погрешна лозинка);
5. Поставена е хардверска и инсталирана софтверска заштитна мрежна бариера(„firewall“), како и рутер помеѓу информатичкиот систем и интерната конекција или која било другаформа на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот;
6.Инсталирана е ефективна и сигурна антивирусна и антиспајвер заштита на информацискиотсистем, која постојано се ажурира заради превентива од непознати и непланирани заканиод нови вируси и спајвери;
7. Инсталирана е ефективна и сигурна антиспам заштита, која постојано се ажурира заради превентивна заштита од спамови и
8. Серверите во Универзитетот се приклучени на енергетска мрежа преку уред за непрекинато напојување.
9. Обезбедување на веб-страницата на Универзитетот со примена на технички мерки со кои го гарантира точниот идентитет на страницата, како и доверливоста на информациите на страницата.

Член 10

Пристап до компјутерот кој содржи софтвер за пресметка на плати на вработените со лични податоци од вработените има само вработеното лице кое е овластено согласно со Правилникот за внатрешна организација и систематизација на работните места на Универзитетот.
Обработка на личните податоци на вработените се врши на компјутерите во Универзитетот до кои пристап имаат само вработените лица кои се овластени согласно со Правилникот за внатрешна организација и систематизација на работните места на Универзитетот.
Обработка на личните податоци на странките во облигационите договори се врши на компјутерите во Универзитетот до кои пристап имаат само вработените лица кои се овластени согласно со Правилникот за внатрешна организација и систематизација на работните места на Универзитетот.
Обработка на личните податоци на студентите се врши на компјутерите во Универзитетот до кои пристап имаат само вработените лица кои се овластени согласно со Правилникот за внатрешна организација и систематизација на работните места на Универзитетот.
Обработка на личните податоци на волонтерите се врши на компјутерите во Универзитетот до кои пристап имаат само вработените лица кои се овластени согласно со Правилникот за внатрешна организација и систематизација на работните места на Универзитетот.
Документите кои содржат лични податоци, по истекот на рокот на чување, согласно со прописите за архивска граѓа, се уништуваат. Документите во хартиена форма кои содржат лични податоци по истекот на рокот на нивното чување се уништуваат на шредер во доволнамера, истите повторно да не бидат употребливи и читливи.
За документите кои се пренесуваат преку електронско комуникациската мрежа, а содржат посебни категории на лични податоци и/или матичен број на граѓанин, задолжително се применуваат технички и организациски мерки кои се класифицирани на стандардно и високо ниво.
Пристапот на вработените до интернет е ограничен. Документите кои содржат лични податоци на вработените во Универзитетот, како и документите со личните податоци на странките во облигационите договори и на волонтеритесе чуваат во заклучени сефови и

плакари, во заклучени простории и пристап до нив имаатвработените кои се овластени за водење на тековните работи согласно со Правилникот за внатрешна организација и систематизација на работните места на Универзитетот.
Личните податоци на студентите кои студираат на Универзитетот се чуваат во заклучени канцеларии и пристап до нив имаат вработените кои се овластени за водење на тековните работи согласно со Правилникот за внатрешна организација и систематизација на работнитеместа на Универзитетот.
Вработеното лице кое ги врши работите во Одделот за правна служба на Универзитетот го известува администраторот на информатичкиот систем за вработување или ангажирање накорисник со право на пристап до информатичкиот систем, за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето, за да му бидат избришани корисничкото име и лозинката.
Вработеното лице кое ги врши работите во Одделот за правна служба на Универзитетот го известува администраторот на информатичкиот систем и при други промени во работниотстатус или статусот на ангажирање на овластеното лице, што има влијание врз нивото надозволениот пристап до информатичкиот систем.

Член 11

Универзитетот води евиденција за корисниците кои имаат авторизиран пристап до документите и информатичкиот систем и има воспоставено постапки за идентификација и проверка на авторизираниот пристап. Оваа евиденција се чува најмалку 5 (пет) години. Во евиденцијата се внесуваат и нивоата на авторизиран пристап на секој вработен, како и име и презиме на корисникот, работната станица од каде се пристапува до информатичкиот 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 на информатичкиот систем. Во евиденцијата се внесуваат и податоци за идентификување на информатичкиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.
Овие операции се контролираат и од страна на офицерот за заштита на личните податоци и истите не може да се деактивираат. Офицерот за заштита на личните податоци врши периодична проверка на податоците, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.
Кога проверката се врши врз основа на корисничко име и лозинка, Универзитетот секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите.
Лозинките се менуваат по изминат временски период што не е подолг од три месеци и се чуваат заштитени со соодветни методи, така што не се разбирливи додека се валидни.
Вработените имаат авторизиран пристап само до личните податоци и информатичко-комуникациската опрема кои се неопходни за извршување на нивните работни задачи.
Универзитетот има воспостевено механизми со кои се оневозможува пристап на вработените до личните податоци и информатичко-комуникациската опрема со права различни од тие за кои се авторизирани.
Универзитетот има воспоставено механизми кои овозможуваат јасна идентификација на секое овластено лице кое пристапило до информатичкиот систем и има можност за проверка на авторизацијата на секое овластено лице.
Администраторот на информатичкиот систем може да доделува, менува или да го одзема авторизираниот пристап до информатичко - комуникациската опрема само во согласност со критериумите кои се утврдени од страна на Универзитетот.
Одредбите од оваа одлука се применуваат при автоматизирана и при рачна обработка на личните податоци што се дел од постојната збиирка на лични лодатоци во Универзитетот.

Член 12

Серверите кои содржат лични податоци, физички се лоцирани и хостирани во Универзитетот во посебна просторија.

Доколку е потребен пристап на друго лице до просторијата во кои се наоѓаат серверите, тогаш тоа лице треба да биде придружувано и надгледувано од лицето од став 1 на овој член.

За просторијата во која се наоѓаат серверите се преземаат мерки за заштита од потенцијални закани, како што се: кражба, пожар, експлозии, чад, вода, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

Член 13

Универзитетот овластува офицер за заштита на личните податоци кој ќе биде одговорен за координација и контрола на постапките и упатстват утврдни со техничките и организациските мерки за безбедување на тајноста и заштитата на обработката на личните податоци.

Член14

Лицата кои се вработуваат или се ангажираат на Универзитетот, пред нивното започнување со работа се запознаваат со прописите за заштита на личните податоци, како и со документацијата за техничките и организациските мерки.

Лицата кои се вработуваат или се ангажираат на Универзитетот, пред нивното започнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

Во изјавата за тајност и заштита на обработката на личните податоци, лицето изјавува дека ќе ги почитува начелата за заштита на личните податоци пред нивниот пристап до личните податоци, ќе вршат обработка на личните податоци согласно со документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци во Универзитетот, освен ако со закон поинаку не е уредено и дека истите ќе ги чуваат како доверливи лични податоци.

Изјавата за тајност и заштита на обработката на личните податоци задолжително се чува во персоналните досиеја на лицата кои се вработуваат или ангажираат.

Изјавата за тајност и заштита на обработката на личните податоци е составен дел на овие Правила.

Универзитетот задолжително врши континуирано информирање на вработените за непосредните обврски и одговорности за заштита на личните податоци.

Член 15

Пристап до документите во хартиена форма кои содржат лични податоци имаат вработените во Универзитетот и други овластени лица во согласност со работните должности утврдени во Правилникот за внатрешна организација и систематизација на работните места наУниверзитетот.

За пристапувањето до документите задолжително се воспоставуваат механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува, како и за пристапот на други лица до документите.

Овластените лица во Универзитетот задолжително го применуваат правилото „чисто биро“ при обработка на личните податоци содржани во документите, за нивна заштита за време на целиот процес на обработката од пристап на неовластени лица.

Копирањето и умножувањето на документи го вршат единствено вработените лица во Универзитетот, согласно со овластувањата утврдени во Правилникот за внатрешна организација и систематизација на работните места на Универзитетот.

За документите кои физички се пренесуваат надвор од работните простории на Универзитетот, задолжително се преземаат мерки за нивна заштита од неовластен

пристап или ракување со личните податоци содржани во документите кои се пренесуваат, така што личните податоци содржани во истите нема да бидат видливи и достапни за трети лица илидруги неовластени лица.

Член 16

Универзитетот обезбедува заштита на својата внатрешна мрежа преку овозможување само на неопходните мрежни функции потребни за обработка на личните податоци, а особено преку:

- управување со Wi-Fi мрежата кое опфаќа јористење на најсовремените методи на криптирање (на пример: WPA2 или WPA2-PSk и со употреба на комплексна лозинка која на определен временски период се менува);
- Wi-Fi мрежата е отворена за употреба на лица кои не се овластени (на пример надворешни посетители) задолжително да биде одвоена од внатрешната мрежа.

Универзитетот врз основа на анализата на ризикот, покрај мерките наведени во ставот (1) од овој член, може да примени и други мерки со кои ќе ја зајакне заштитата на својата внатрешна мрежа.

Член 17

Универзитетот има своја веб-страница треба да примени технички мерки со кои ќе го гарантира точниот идентитет на страницата (pharming prevention), како и доверливоста на информациите што ги испраќа или ги собира преку веб-страницата, и тоа особено преку следните мерки:

- имплементација на криптографски протокол (TLS заменувајќи го SSL) на сите веб страници на контролорот (ако има повеќе од една), јористејќи ја единствено најновата верзија и со проверка на неговата правилна имплементација;
- задолжителна употреба на криптографии протокол (TLS) за сите страници од веб страницата,
- ограничување на портите за комуникација на оние кои се строго потребни за правилно функционирање на инсталираните апликации. Ако веб серверот прифаќа само врски со HTTPS протокол, само P мрежен сообраќај кој влегува преку портата 443 е дозволен, а сите други пристапни порти мора да бидат блокирани;
- обезбедување дека само овластени лица ќе можат да имаат пристап до алатките и административните интерфејси, при што особено да се ограничи употребата да биде достапна само до овластените лица со администраторски привилегии кои се дел од тимот одговорен за информатичката технологија и само за административни активности што се неопходни; и
- ако се јористат колачиња што не се потребни од услугата, контролорот обезбедува претходна согласност од интернет корисникот откако ќе го извести корисникот, а пред да се депонира колачето;

Универзитетот кој има своја веб-страница не треба да применува практики кои го зголемуваат ризикот од можна злоупотреба, несакана (случајна) или намерна неовластена обработка на личните податоци, а особено:

- да не пренесува лични податоци преку URL без примена на протокол за криптирање (на пример идентификатори или лозинки);
- користење на небезбедни услуги;
- употреба на сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страници, пристап до електронски пораки и слично;
- поставување на базите на податоци на сервери кои се директно достапни преку интернет; и

- споделување и употреба на корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.

Член 18

Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и обврските и одговорностите на администраторот на информатичкиот систем се дефинирани и утврдени во Правилник за определување на обврските и одговорностите на администраторот на информатичкиот систем и на овластените лица.

Член19

Начинот на евидентирање на секој инцидент, времето кога се појавил, корисникот кој го пријавил, на кого е пријавен и преземените мерки, се уредени со Правилник за пријавување, реакција и санирање на инциденти.

Член20

Со медиумите се овозможува идентификација и евидентирање на категориите на лични податоци и истите се чуваат на локација до која пристап имаат само овластените лица.
Универзитетот има воспоставено систем за евидентирање на медиумите кои се примаати испраќаат со што е овозможена директна и/или индиректна идентификација на видот на медиумот кој е примен, датум и време на примање, испраќач, број на медиуми кои се примени, вид на документ кој е снимен на медиумот, начин на испраќање на медиумот и име и презимена лицето овластено за приемот на медиумот.
Пренесувањето на медиумите надвор од работните простории се врши само со претходно писмено одобрување од страна на овластеното лице на Универзитетот и се преземаат ситемерки за да се спречи неовластено обработување на податоците снимени на нив.
Постапките и процедурите за управувањето, уништувањето, како и за бришењето или чистењето на медиумот се определени со Правилник за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите.

Член 21

Постапките и процедурите за правење на сигурносни копии, како и начинот на чување се регулирани со Правилник за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци.

Член 22

Вработените лица во ИТ секторот на Универзитетот се овластени лица кои ќе бидат одговорни за координација и контрола на постапките и упатствата утврдени во документацијата за техничките и организациските мерки на Универзитетот.

Член 23

Личните податоци кои ќе се пренесуваат преку електронско - комуникациска мрежа од Универзитетот до Управата за јавни приходи, а кои содржат и единствен матичен број на вработените во Универзитетот, се криптирани, односно заштитени со соодветни мерки кои гарантираат дека податоците нема да бидат читливи при преносот.

Член 24

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

Универзитетот врши надворешна контрола на информатичкиот систем и информатичката инфраструктура на секои три години, а внатрешна контрола секоја година.
Надворешната контрола се врши преку обработка на документи од страна на независно правно лице.
Во извештајот од извршената контрола, задолжително 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, наведени секонстатираните недостатоци, како и предложените неопходни корективни или дополнителни мерки за нивно отстранување. Во извештајот се содржани и податоците и фактите врз основа на кои е изготвено мислењето и се предложени мерките за отстранување на констатираните недостатоци. Извештајот се анализира од страна на офицерот за заштита на личните податоци и тој доставува предлози до Универзитетот за преземање на потребните корективни или дополнителни мерки за отстранување на констатираните недостатоци.

IV. ВИСОКО НИВО

Член 25

Универзитетот врз основа на анализата на ризикот воведува и применува дополнителни мерки за безбедност на личните податоци со кои ќе демонстрира дополнителна усогласеност со прописите и добрите практики за заштита на личните податоци.

Член 26

Универзитетот задолжително врши тестирање на информацискиот систем пред неговото имплементирање или по извршените промени со цел да се провери дали системот обезбедува безбедност на личните податоци согласно со прописите за заштита на личните податоци.
Тестирањето од став (1) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци.

Член 27

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.

V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 28

Оваа Политика влегува во сила со денот на објавувањето во „Универзитетски билтен“ на Универзитетот за информатички науки и технологии „Свети Апостол Павле“Охрид, а ќе биде објавен и на веб-страната на Универзитетот.
Со влегување во сила на оваа Политика престанува да важи Правилникот за техничките и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци на Универзитетот за информатички науки и технологии „Свети Апостол Павле“Охрид, арх. бр. 01-763/1 од 28.06.2013 година.

Претседател на Универзитетски сенат
Вонр. проф. д-р Атанас Христов с.р.

Врз основа на Законот за заштита на личните податоци („Службен весник на Република Северна Македонија “ бр. 42/2020) и одредбите од член 31 став 4 од Правилник за безбедност и заштита на личните податоци („Службен весник на Република Северна Македонија” бр.122/20), а согласно документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци на _____, на _____, 20__ година ја давам следната

И З Ј А В А
за обезбедување тајност и заштита на обработката на личните податоци

Јас долупотпишаниот/ната,_____
(Име и Презиме)
распореден/а на работното место _____ во _____ согласно
(одделение/факултет)
Правилникот за безбедност и обработка на личните податоци и документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци на _____ се обврзувам дека
(назив на контролорот односно обработувачот

- **ќе ги почитувам начелата поврзани со обработката на личните податоци;**
- **ќе ги применувам техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци соодветно на ризикот и ќе ги чувам како доверливи личните податоци, како и мерките за нивна заштита;**
- **ќе вршам обработка на личните податоци согласно упатствата добиени од _____;**
(назив на контролорот односно обработувачот)

- **на трети лица надвор од _____ и на други**
(назив на контролорот односно обработувачот)
лица од _____, нема да издавам било
(назив на контролорот односно обработувачот)

каков податок од збирките на лични податоци или било каков друг личен податок кој ми е достапен и кој сум го дознал или ќе го дознам при работата во _____.

(назив на контролорот односно обработувачот)

Потпис,

_____