



Република Северна Македонија

**Министерство за
јавна администрација**



РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT
МИНИСТЕРСТВО ЗА ЈАВНА АДМИНИСТРАЦИЈА
MINISTRIA E ADMINISTRATËS PUBLIKE

Бр.-Nr. 16-2392/1

12.06 20 26 год.-viti
Скопје - Shkup

Врз основа на член 28 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20, 294/21 и 101/25), Министерот за јавна администрација, ја донесе следната

**ПОЛИТИКА ЗА ВОСПОСТАВУВАЊЕ НА СИСТЕМ ЗА ЗАШТИТА НА ЛИЧНИТЕ
ПОДАТОЦИ ВО МИНИСТЕРСТВОТО ЗА ЈАВНА АДМИНИСТРАЦИЈА**

I. Цел и опсег на Политиката

Политиката за воспоставување на систем за заштита на личните податоци (во натамошниот текст – Политика), има за цел да го утврди **начинот** на постапување на Министерството за јавна администрација (во натамошниот текст: министерството), во својство на Контролор, како и на неговите вработени и ангажирани лица кои ги обработуваат личните податоци, со цел да се исполнат **стандардите и начелата** поврзани со обработката на личните податоци. Притоа со Политиката се опфатени и **процесите на управување со системот** за заштита на личните податоци при нивната обработка од страна на министерството.

Министерството во рамките на својот делокруг на работење, а со цел извршување на својата основна дејност во доменот на прибирање, обработка, одржување, управување, користење, дистрибуција, издавање и единствен пристап кон податоците, врши собирање, чување и обработка на лични податоци.

Од аспект на заштита на обработката на личните податоци, министерството е Контролор на лични податоци, а субјекти на лични податоци се физичките и правни лица кои во соодветна и пропишана постапка имаат потреба да ги остварат своите права и обврски за коишто министерството има законски утврдена надлежност за постапување. Оваа Политика се применува и се однесува на обработката на сите документи и записи што содржат лични податоци и коишто се креирани во писмена, електронска и видео форма.

При обработката на личните податоци задолжителна е примена на законските и подзаконските прописи за заштитата на личните податоци, особено на Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20, 294/21

и 101/25) и на подзаконските акти донесени врз основа на истиот. Обработката на личните податоци се врши со задолжително почитување на начелата за законитост, правичност и транспарентност.

Личните податоци безбедно се чуваат од губење, уништување, фалсификување и неавторизиран пристап. Единствено авторизирани вработени имаат пристап до нив.

Личните податоци се чуваат во форма што овозможува идентификација на субјектот на личните податоци, не подолго од што е потребно да се исполнат целите поради кои податоците се собрани за натамошна обработка, по што истите се бришат и уништуваат.

Заради спречување на неовластен пристап и злоупотреба на личните податоци, во континуитет се преземаат сите потребни технички и организациски мерки за заштита на личните податоци.

II. Законски основ на збирки на лични податоци што се обработуваат

Во министерството е имплементиран систем за технички и организациски мерки што се применуваат заради обезбедување на безбедност и заштита на обработката на личните податоци и заради оценка на нивната адекватност со видот и обемот на работните процеси што ги врши Министерството за јавна администрација.

Во министерството се обработуваат следните збирки (категории) на лични податоци:

1. Заради спроведување на конкретни права и обврски врз основа на работен однос, односно од областа на трудовото право:

- име и презиме на вработените во министерството;
- датум и место на раѓање;
- извод од матична книга на родени;
- извод од државјанство;
- општина на раѓање;
- место на раѓање;
- лични документи (вид на документ, број на документ, датум на издавање, датум на важност, место на издавање на документот);
- адреса на живеење или престојување;
- место на живеење;
- општина на живеење;
- единствен матичен број на вработените;
- број на трансакциски сметки на вработените;
- држава;
- припадност на заедница;

- пол;
- брачен статус (датум на брачен статус, сопруг/а (ЕМБГ));
- смрт (датум и место);
- е-адреса;
- податоци (дипломи, уверенија) за образованието, стручните квалификации и работните компетенции;
- податоци за годишните оценки;
- податоци за висината на платата и надоместоците од плата и
- други податоци за вработените.

Збирка за евиденција на плати на вработените со следните категории лични податоци што се собираат и обработуваат:

а) Податоци за работното време на работникот и за користење на работното време, и тоа:

- можен број на работни часови за полно и за скратено работно време;
- вкупно остварени работни часови за полно и за скратено работно време;
- неизвршени часови за коишто се прима надомест на плата од средствата на работодавачот, и тоа за: привремена спреченост на работа според прописите на здравствено осигурување; стручно образование и усовршување; и прекин на работа поради штрајк;
- вкупно неизвршени часови за коишто се прима надомест од средствата на друг работодавач;
- вкупно неизвршени часови за коишто се прима надомест на плата од средствата за здравствено осигурување, и тоа за: часови за привремена спреченост за работа поради болест, повреда и други причини; часови на отсуство од работа поради болест, повреда и други причини; часови на отсуство од работа, поради бременост, раѓање и мајчинство; и работа со половина од полното работно време на родителот со потешко хендикепирано дете; и неизвршени часови за коишто не се прима надомест на плата; и
- часови на работа подолго од работното време.

б) Податоци за бруто/нето платите на работникот:

- исплата на бруто-плата и тоа за работа: со полно работно време; со скратено работно време; и подолго од полното работно време;
- исплата на нето-плата и тоа за работа: со полно работно време; со скратено работно време; и подолго од полното работно време;

- најниска бруто и нето плата;
- додаток на плата; и
- надоместоци на плата, и тоа од средствата на работодавачот и од средствата на друг работодавач.

в) Надоместоци и други примања на работникот од работодавачот, и тоа за:

- регрес за годишен одмор; испратнина; отпремнина при заминување во пензија; солидарна помош и надомест за одвоен живот.

г) Податоци за платените придонеси и даноци од плата.

2. Заради спроведување на постапки за вработување во министерството, се обработуваат личните податоци на кандидатите за вработување, и тоа:

- име, име на родител и презиме на кандидатот во министерството;
- датум и место на раѓање;
- место на раѓање;
- адреса;
- место на живеење;
- држава;
- телефон и е-адреса;
- податоци за завршеното образование;
- податоци за работното искуство (за работодавач и за работното место);
- податоци за стажот и
- други податоци за вработените.

3. Лични податоци на странките и трети лица при водење на управни постапки и постапки по претставки и предлози, согласно Законот за вработени во јавен сектор, Законот за административни службеници, Законот за инспекциски надзор, Закон за организација и работа на органите на државната управа, Законот за заштита на лични податоци, Законот за општа управна постапка, Закон за користење на податоците од јавниот сектор, Закон за постапување по претставки и предлози, Законот за управна инспекција, Закон за прекршоците, Закон за работните односи, Закон за прибавување и размена на докази и податоци по службена должност, Закон за воведување на систем за управување со квалитет и заедничка рамка на работењето и давањето на услуги во државната служба, Законот за стручно усовршување и обука на административните службеници и лични податоци кои што се користат во информациониот систем за управување со човечки ресурси (ИСУЧР):

- име и презиме;

- адреса на живеење или престојувалиште;
- единствен матичен број на граѓанинот;
- телефонски броеви и е-маил адреси;
- работно место;
- даночен број;
- жиро-сметка;
- податоци за вработување; и
- други податоци потребни за изведување како доказ во постапките согласно закон.

III. Безбедност при обработка на личните податоци

Системот за технички и организациски мерки за обезбедување на безбедност и заштита на обработката на личните податоци во министерството се состои од следните механизми имплементирани со донесување и изготвување на соодветни акти:

1. Донесување на План за технички и организациски мерки за обезбедување на безбедност и заштита на обработката на личните податоци;
2. Донесување на Процедура за технички и организациски мерки за обезбедување на безбедност и заштита на обработката на личните податоци;
3. Донесување на Процедура за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица;
4. Донесување на Процедура за пријавување, реакција и санирање на инциденти;
5. Донесување на Процедура за правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
6. Донесување на Процедура за правото на исправка на личните податоци од страна на субјектите на личните податоци.
7. Донесување на Процедура за начинот на уништување на документите, бришење и чистење на медиумите;
8. Донесување на Процедура за начинот на вршење на видеонадзор во Министерството за јавна администрација;
9. Изготвување на Анализа на целите за кои се поставува видеонадзорот во Министерството за јавна администрација;
10. Донесување на Методологија влијанието на заштитата на личните податоци;

11. Изготвување на Анализа на ризик на активностите за обработка на личните податоци;
12. Донесување на Политика со опис на техничките и организациските мерки на информацискиот систем и информатичката инфраструктура;
13. Изготвување на Преглед на порти на заштитниот ѕид (firewall);
14. Донесување на внатрешни акти и посебни овластувања за обработка на личните податоци со коишто се утврдени правата, обврските и одговорностите на сите кои имаат пристап до информацискиот систем на Министерството за јавна администрација на којшто се врши обработката на личните податоци; и
15. Донесување и изготвување и на други акти поврзани со заштитата и безбедноста на личните податоци.

IV. Поделба на должности и одговорности

Вработените и ангажираните лица во министерството се должни секој во рамките на своите работни задачи да ги почитуваат и применуваат овие интерни акти.

Офицерот за заштита на личните податоци во министерството врши редовна проценка на потребата за изготвување и донесување на нови интерни акти или промена на старите од аспект на нивно усогласување со прописите за заштита на личните податоци.

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

Образецот на изјавата од став 3 на овој член е дадена во прилог на оваа Политика и е нејзин составен дел (Прилог бр. 1).

V. Офицер за заштита на личните податоци

Во министерството е определено и овластено лице за заштита на личните податоци, односно офицер за заштита на личните податоци, кое е задолжено:

- да го информира и советува Контролорот или обработувачот и вработените во министерството кои вршат обработка соодветно на нивните обврски според одредбите од Законот за заштита на личните податоци;
- да ја следи усогласеноста со Законот за заштита на личните податоци со други засегнати закони кои се однесуваат на заштитата на личните податоци во Република Северна Македонија, како и со политиките на Контролорот или обработувачот во однос на заштитата на личните податоци, вклучувајќи распоредување на одговорности, подигнување на свеста и обучување на вработените кои учествуваат во операциите на обработка, како и вршење на ревизии за заштита на личните податоци;
- каде што е потребно, да дава совети во однос на процената на влијанието на заштитата на личните податоци и го следи извршувањето на процената во согласност со членот 39 од Законот за заштита на личните податоци;
- да соработува со Агенцијата за заштита на личните податоци;
- да дејствува како контакт точка за Агенцијата во однос на прашањата поврзани со обработката, вклучувајќи ја претходната консултација од членот 40 од Законот за заштита на личните податоци, како и советување според потребите за сите други прашања;
- при извршувањето на своите работи да ги земе во предвид ризиците поврзани со операциите на обработката, како и природата, обемот, контекстот и целите на обработката кај Контролорот и одговара пред Министерот за јавна администрација.

Решението за определување на овластено лице за заштита на личните податоци е составен дел на оваа политика (Прилог бр.2).

VI. Одговорно лице за сигурност на информацискиот систем

Во министерството е определено и овластено лице за сигурност на информацискиот систем (администратор на информацискиот систем) кое е задолжено:

- за планирање и примена на техничките и организациските мерки за безбедност на личните податоци утврдени од страна на контролорот;
- за контрола на обезбедувањето тајност и заштита на обработката на личните податоци;
- да ги доделува, менува, одзема и ажурира привилегии за авторизираниот пристап до личните податоци и информатичко комуникациската опрема на одреден

временски период во зависност од фреквенцијата на статусни промени во врска со вработувањето, распоредувањето, ангажирањето и/или престанокот на вработувањето, а најмалку еднаш годишно;

- да доделува корисничко име и лозинка (за прва најава), како и врши бришење на корисничките имиња и лозинки, или ги заклучува за натамошен пристап во согласност со критериумите на контролорот;
- да ја хостира посебната електронска пошта за контакт и пријавување на инциденти или појави на невообичаени настани што можат да влијаат на информациите и комуникацијата на системите на министерството (доколку има ваква електронска пошта, а согласно анализата на ризик);
- да управува со системот за евиденција за пристап до информацискиот систем;
- да го известува раководството на министерството за секоја аномалија или безбедносен инцидент, веднаш, а најдоцна во рок од 24 часа од моментот на инцидентот;
- со одобрение од раководството, а согласно состојбата и видот на амортизираниот медиум да врши негово уништување (на пример УСБ, ЦД...) или бришење на податоците (на пример: хард-диск, лаптоп...);
- да овозможува пристап до интернет преку овластен провајдер согласно анализата на ризик и согласно одлуката на раководството го ограничува пристапот до интернет со блокирање на сите несуштински услуги и сервиси;
- да одговара за сервер просторијата и оперативните сервери на кои се врши централна обработка на личните податоци од страна на сите вработени во министерството;
- да се грижи за примена на мерки за минимизирање на ризиците од можни напади (на пример од напади преку инјектирање на SQL кодови, скрипти – cross site script attack, Denial of Service Attack – DOS напад и сл.);
- во случај на настанат физички или технички инцидент кој ја нарушува информациската сигурност на системите, во соработка со вработените да го менаџира справувањето со инцидентот и ги презема сите мерки неопходни за повторно воспоставување на достапноста на личните податоци;
- да врши редовно тестирање на функционалноста на сигурносните копии за што во соработка со офицерот за заштита на личните податоци изработува План за обезбедување на континуитет;
- да ја проверува функционалноста на алармниот систем за детекција на движење против упад и превенција од кражба (доколку има ваков систем);
- да ги информира вработените за: воспоставениот систем за евиденција за пристап до информацискиот систем (логови), специфичните ризици поврзани со

користење на преносливите медиуми и утврдените процедури за намалување на овие ризици поврзани со користење на преносливите медиуми и утврдените процедури за намалување на овие ризици и техничките и организационите мерки кои се однесуваат на извршувањето на нивните конкретни обврски и одговорности;

- да врши контрола на операциите кои овозможуваат евидентирање на секој пристап до информацискиот систем – logs, како и во однос на техничкото оневозможување за нивно деактивирање;
- да се грижи за примена на сите технички решенија во согласност со најсовремените технолошки достигнувања за што во соработка со офицерот за заштита на личните податоци му предлага на раководството соодветни предлог унапредувања на процесите и информацискиот систем во целина;
- при извршувањето на своите работи да ги земе во предвид ризиците поврзани со операциите на обработката, како и природата, обемот, контекстот и целите на обработката во министерството.

Решението за определување на овластено лице сигурност на информацискиот систем (администратор на информацискиот систем) е составен дел на оваа политика (Прилог бр.3).

VII. Улогата на организациските единици во рамки на министерството

Организациските одговорности за обезбедување на услови за имплементација на техничките и организациските мерки и контроли што се однесуваат на нивниот делокруг на работење, во министерството се хиерархиски определени со Правилникот за систематизација на работните места, распоредени во тринаесет сектори и три независни одделенија, односно:

1. Сектор за реформа на јавната администрација со: Одделение за креирање и анализа на политики во областа на РЈА и Одделение за координација на СРЈА;
2. Сектор за поддршка на институциите од јавниот сектор со: Одделение за годишни планови за вработување и Одделение за систематизации;
3. Сектор за развој и управување со човечките ресурси во јавната администрација со: Одделение за координација на мрежата за управувањето со човечките ресурси и Одделение за инклузивност, анализа, планирање и иновации во јавниот сектор;
4. Сектор за стручно усовршување на административните службеници со Одделение за креирање на политики за обука и Одделение за координација на обуки;

5. Сектор за нормативно-правни работи со: Одделение за нормативно-правни работи, Одделение за примена на ЗИН и ЗОУП и Одделение за координација на ПВР и ОСР;
6. Сектор за интеграција во ЕУ и меѓународна соработка со: Одделение за интеграција во ЕУ и меѓународна соработка и Одделение за ИПА;
7. Сектор за општи и заеднички работи и јавни набавки со: Одделение за канцелариско и архивско работење, Одделение за општи работи и Одделение за јавни набавки;
8. Сектор за финансиски прашања со Одделение за буџетска координација, Одделение за буџетска контрола и Одделение за сметководство и плаќања;
9. Сектор за односи со јавност и поддршка на работата на Кабинетот на министерот со: Одделение за поддршка на Кабинетот на министерот и протоколарни активности и Одделение за односи со јавност;
10. Сектор за апликативно одржување на системите за организациска поддршка и развој на ресурсите на јавната администрација со: Одделение за апликативна поддршка на ИКТ системи и Одделение за техничка поддршка, администрирање и развој на ИСУЧР;
11. Сектор за вршење на инспекциски надзор исток со: Одделение за инспекциски надзор за североисточен регион и Одделение за инспекциски надзор за југоисточен регион;
12. Сектор за инспекциски надзор запад со: Одделение за инспекциски надзор за северозападен регион и Одделение за инспекциски надзор во југозападен регион;
13. Сектор за општи и заеднички работи и административно-техничка поддршка на инспекторатот со: Одделение за човечки ресурси и административно-техничка поддршка на инспекторатот и Одделение за финансии и финасиски прашања за поддршка на инспекторатот;
14. Одделенија надвор од сектори: Одделение за внатрешна ревизија, Одделение за стратешко планирање и Одделение за управување со човечки ресурси во министерството.

Одговорностите за обезбедување на услови за имплементација на техничките и организациските мерки и контроли од страна на вработените административни службеници во министерството, а коишто се однесуваат на заштитата и безбедноста на обработката на личните податоци, се определени од најниското кон највисокото ниво на работните места според нивните категории и нивоа.

VIII. Пристап на трети лица

Пристапот на трети лица е обезбеден со сигурноста на информацискиот систем со којшто се врши обработка на личните податоци. Притоа се преземени технички и организациски мерки заради обезбедување на безбедност соодветно на ризикот во случај кога станува збор за

пристап од трети лица, како и за физички пристап на лица во службените простории на министерството.

IX. Ревизија на Политиката

Ревизијата на оваа Политика е потребно да се врши по потреба, а задолжително во случај кога се менуваат актите за организација и систематизација на работните места во министерството.

Х. Завршна одредба

Оваа Политика влегува во сила и ќе се применува со денот на нејзиното донесување.

Министер за јавна администрација
Горан Минчев



Прилог 1

Врз основа на одредбите од Законот за заштита на личните податоци Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“, бр. 42/2020, 294/2021 и 101/2025) и Правилникот за безбедност на обработката на личните податоци податоци („Службен весник на Република Северна Македонија“ бр. 122/2020), на ден _____ година, ја давам следната

ИЗЈАВА

за обезбедување тајност и заштита на обработката на личните податоци

Јас, долупотпишаниот/ата _____, распореден/а на работното место _____ во Министерството за јавна администрација, согласно со Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“, бр. 122/2020), а во врска со Политиката за воспоставување на систем за заштита на личните податоци во Министерството за јавна администрација, се обврзувам дека:

- 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; и
- ќе вршам обработка на личните податоци согласно упатствата добиени од Министерството за јавна администрација.

ИЗЈАВИЛ:

(потпис)

Прилог 2

Врз основа на член 41 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“, бр. 42/2020, 294/2021 и 101/2025), Министерот за јавна администрација, на ден _____ година, го донесе следното

РЕШЕНИЕ

за определување на овластено лице за заштита на личните податоци

1. Се определува _____, распореден/а на работното место _____ во Министерството за јавна администрација за овластено лице за заштита на лични податоци, односно офицер за заштита на личните податоци во Министерството за јавна администрација.

2. Се задолжува лицето од точка 1 на ова решение да ги врши следните работи:

- го информира и советува контролорот Министерството за јавна администрација или обработувачот и вработените во Министерството за јавна администрација кои вршат обработка соодветно на нивните обврски според одредбите од Законот за заштита на личните податоци;
- ја следи усогласеноста со Законот за заштита на личните податоци со други засегнати закони кои се однесуваат на заштитата на личните податоци во Република Северна Македонија, како и со политиките на контролорот или обработувачот во однос на заштитата на личните податоци, вклучувајќи распоредување на одговорности, подигнување на свеста и обучување на вработените кои учествуваат во операциите на обработка, како и вршење на ревизии за заштита на личните податоци;
- каде што е потребно, дава совети во однос на процената на влијанието на заштитата на личните податоци и го следи извршувањето на процената во согласност со членот 39 од Законот за заштита на личните податоци;
- соработува со Агенцијата за заштита на личните податоци;
- дејствува како контакт точка за Агенцијата во однос на прашањата поврзани со обработката, вклучувајќи ја претходната консултација од членот 40 од Законот за заштита на личните податоци, како и советување според потребите за сите други прашања.

3. Овластеното лице е должно при извршувањето на своите работи да ги зема во предвид ризиците поврзани со операциите на обработката, како и природата, обемот, контекстот и целите на обработката кај контролорот и одговара пред Министерот за јавна администрација.

5. Ова решение влегува во сила со денот на донесувањето.

Министер за јавна администрација
Горан Минчев



Прилог 3

Врз основа на член 55 став 1 од Законот за организација и работа на органите на државната управа („Службен весник на Република Македонија“ бр. 58/00, 44/02, 82/08, 167/10, 51/11 и „Службен весник на Република Северна Македонија“ бр. 96/19, 110/19 и 121/24), а во врска со одредбите од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“, бр. 42/2020, 294/2021 и 101/2025) и Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“, бр. 122/20), Министерот за јавна администрација, го донесе следното

РЕШЕНИЕ

за определување на овластено лице за сигурност на информацискиот систем (администратор на информацискиот систем)

1. Се определува _____, распореден/а на работното место _____ во Министерството за јавна администрација, за администратор на информацискиот систем како лице задолжено за сигурност на информацискиот систем во Министерството за јавна администрација.

2. Лицето од точка 1 на ова решение се задолжува да ги врши особено следните работи:

- планирање и примена на техничките и организациските мерки за безбедност на личните податоци утврдени од страна на контролорот;
- контрола на обезбедувањето тајност и заштита на обработката на личните податоци;
- ги доделува, менува, одзема и ажурира привилегии за авторизираниот пристап до личните податоци и информатичко комуникациската опрема на одреден временски период во зависност од фреквенцијата на статусни промени во врска со вработувањето, распоредувањето, ангажирањето и/или престанокот на вработувањето, а најмалку еднаш годишно;
- доделува корисничко име и лозинка (за прва најава), како и врши бришење на корисничките имиња и лозинки, или ги заклучува за натамошен пристап во согласност со критериумите на контролорот;
- ја хостира посебната електронска пошта за контакт и пријавување на инциденти или појави на невообичаени настани што можат да влијаат на информациите и комуникацијата на системите на Министерството за јавна администрација (доколку има ваква електронска пошта, а согласно анализата на ризик);
- управува со системот за евиденција за пристап до информацискиот систем;
- го известува министерот на Министерството за јавна администрација за секоја аномалија или безбедносен инцидент, веднаш, а најдоцна во рок од 24 часа од моментот на инцидентот;
- со одобрение од министерот, а согласно состојбата и видот на амортизираниот медиум врши негово уништување (на пример УСБ, ЦД...) или бришење на податоците (на пример: хард-диск, лаптоп...);

- овозможува пристап до интернет преку овластен провајдер согласно анализата на ризик и согласно одлуката на раководството го ограничува пристапот до интернет со блокирање на сите несуштински услуги и сервиси;
- одговорен е за сервер просторијата и оперативните сервери на кои се врши централна обработка на личните податоци од страна на сите вработени во Министерството за јавна администрација;
- се грижи за примена на мерки за минимизирање на ризиците од можни напади (на примерод напади преку инјектирање на SQL кодови, скрипти – cross site script attack, Denial of Service Attack – DOS напад и сл.);
- во случај на настанат физички или технички инцидент кој ја нарушува информациската сигурност на системите, во соработка со вработените го менаџира справувањето со инцидентот и ги презема сите мерки неопходни за повторно воспоставување на достапноста на личните податоци;
- врши редовно тестирање на функционалноста на сигурносните копии за што во соработка со офицерот за заштита на личните податоци изработува План за обезбедување на континуитет;
- ја проверува функционалноста на алармниот систем за детекција на движење против упад и превенција од кражба (доколку има ваков систем);
- ги информира вработените за: воспоставениот систем за евиденција за пристап до информацискиот систем (логови), специфичните ризици поврзани со користење на преносливите медиуми и утврдените процедури за намалување на овие ризици поврзани со користење на преносливите медиуми и утврдените процедури за намалување на овие ризици и техничките и организационите мерки кои се однесуваат на извршувањето на нивните конкретни обврски и одговорности;
- врши контрола на операциите кои овозможуваат евидентирање на секој пристап до информацискиот систем – logs, како и во однос на техничкото оневозможување за нивно деактивирање;
- се грижи за примена на сите технички решенија во согласност со најсовремените технолошки достигнувања за што во соработка со офицерот за заштита на личните податоци му предлага на раководството соодветни предлог унапредувања на процесите и информацискиот систем во целина.

3. Администраторот е должен при извршувањето на своите работи да ги зема во предвид ризиците поврзани со операциите на обработката, како и природата, обемот, контекстот и целите на обработката кај Министерството за јавна администрација.

4. Ова решение влегува во сила со денот на донесувањето.

Министер за јавна администрација
Горан Минчев

