Република Северна Македонија

Дирекција за безбедност
на класифицирани информации

Бр. 02- 1039/7

Скопје, 30. 11 2024 година

Врз основа на член 75 став 1 од Законот за класифицирани информации(*) („Службен весник на Република Северна Македонија“ бр. 275/19), член 55 став 2 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), а во врска со член 119 и 120 од Законот за заштита на личните податоци(*) („Службен весник на Република Северна Македонија“ бр. 42/20) и согласно член 21 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), директорот на Дирекцијата за безбедност на класифицирани информации донесе

ПРАВИЛНИК
ЗА НАЧИНОТ НА ПРЕВЕНИРАЊЕ И УПРАВУВАЊЕ СО ИНЦИДЕНТИ КОИ ЈА НАРУШУВААТ ДОВЕРЛИВОСТА, ИНТЕГРИТЕТОТ ИЛИ ДОСТАПНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 1

Со овој правилник се пропишува начинот на превенирање и управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци во Дирекцијата за безбедност на класифицираните информации (во натамошниот текст: Дирекцијата).

Дефиниција

Член 2

Во смисла на овој правилник:

- „инцидент“ е секое нарушување на доверливоста, интегритетот или достапноста на личните податоци, вклучително и по информацискиот систем на којшто се обработуваат личните податоци;
- „управување со инциденти“ опфаќа пријавување, реакција, санирање и евиденција на инцидентите.

Превенирање на инциденти

Член 3

Дирекцијата ги презема следните мерки и контроли за превенирање на инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци:

- користење на непрекинато напојување за да се заштити опремата што се користи за обработка на личните податоци;
- едновремена употреба на повеќе уреди во низа за зачувување на личните податоци;
- заштита од пожар, експлозии, прашина, вода, кражба, пречки во напојување со електрична енергија, електромагнетно зрачење во просторијата во којашто се сместени серверите;
- во случај на прекин на напојување со електрична енергија, системот треба да биде обезбеден со уред за непрекинато напојување (UPS) како секундарен механизам;
- инсталирање на алармни уреди против упад и нивна периодична проверка;
- обезбеден пристап до просториите во коишто се чуваат безбедносните клучеви и шифрите за аларм;
- контрола за пристап до сервер-собата;
- ажуриран список на лица или категории на лица кои се овластени да влезат во просториите каде што се чува опрема на којашто се врши обработка на лични податоци;
- воспоставување на правила и методи за контрола на пристапот на посетителите во Дирекцијата и тоа минимум со придружба од едно лице на посетителите надвор од утврдена локација за прием на странки;
- одржување на сервер-собата (климатизација, инсталација на UPS уред, итн.);
- применување на политиката за „чист екран и чисто биро“;
- чување на документите во хартиена форма на начин што ќе оневозможи пристап до истите од страна на неовластено лице (на пр. во ормари за чување документи со клуч до кои пристап има овластеното лице за обработка на податоците).

Пријавување на инцидент

Член 4

(1) Секое овластено лице е должно веднаш да го пријави инцидентот кај офицерот а заштита на личните податоци.

(2) Во случај на инцидент поврзан со информацискиот систем на кој што се врши обработка на лични податоци, корисникот кој го забележал инцидентот е

должен веднаш да го пријави инцидентот кај администраторот на информацискиот систем.

(3) Пријавување на инцидентот од ставот (2) на овој член се врши во електронска и/или во писмена форма, пришто се наведуваат следните податоци за инцидентот:

- време на настанување на инцидентот;
- траење и престанување на инцидентот;
- место во информацискиот систем каде што се појавил инцидентот;
- податок или проценка на обемот, односно опсегот на инцидентот;
- име и презиме на овластеното лице коешто го пријавува инцидентот;
- име и презиме на овластените лица до коишто е поднесена пријавата за инцидентот.

(4) Во функција на побрзо преземање мерки за управување со настанатиот инцидент, се препорачува овластеното лице што го пријавува инцидентот, покрај пријавата во електронска и/или во писмена форма, и телефонски да го извести администраторот на информацискиот систем за поднесената пријава за инцидент.

Реакција во случај на пријавен инцидент

Член 5

(1) По приемот на пријавата за инцидентот, администраторот на информацискиот систем го известува директорот на Дирекцијата и веднаш започнува со санирање на инцидентот, врши проценка на причините за појавување на инцидентот, како и утврдување на тоа дали и кои мерки треба да се преземат за евентуално дополнително санирање и за спречување на негово повторување во иднина.

(2) Доколку се работи за инцидент што се повторува, администраторот на информацискиот систем е должен да преземе мерки кои ќе гарантираат трајно отстранување на ризикот за настанување на инцидентот.

(3) Во случај на инцидент за којшто е потребна стручна помош од надворешни лица, администраторот на информацискиот систем во координација со офицерот за заштита на личните податоци, ги презема сите мерки за заштита личните податоци и информациите што се обработуваат на информацискиот систем.

Санирање на инциденти

Член 6

(1) Инцидентот може да го санира само стручно лице овластено за таа цел од страна на директорот на Дирекцијата.

(2) По спроведената постапка за санирање на инцидентот, овластеното лице од ставот (1) на овој член изготвува извештај за реакција по пријавениот инцидент.

(3) Во случај кога заради санација е потребно овластеното лице да пристапи до персоналните компјутери или серверот, тогаш датотеките во кои се чуваат и обработуваат личните податоци не треба да бидат достапни за него.

(4) Доколку при санацијата на инцидентот се јави потреба од влегување во датотеките со лични податоци, тогаш корисникот на чиешто работно место настанал инцидентот го внесува своето корисничко име и лозинка без притоа да дозволи овластеното лице за санирање да ја забележи/открие лозинката.

(5) Во случај на откривање на лозинката, по завршување на постапката за санација на инцидентот, лозинката се уништува и на корисникот му се овозможува креирање на нова лозинка.

(6) Во случај ако при санација на инцидентот овластеното лице сепак дојде во контакт со личните податоци, тоаш тоа лице задолжително ја потполнува и потпишува Изјавата за тајност и заштита на обработката на личните податоци.

(7) За време на санацијата на инцидентот, покрај овластеното лице за санирање задолжително е присуството на корисникот на персоналниот компјутер, а во случај на инцидент на серверот, задолжително е присуството на администраторот на информацискиот систем кој има право на пристап до серверот.

(8) Ако за време на санацијата на инцидентот дојде до оштетување или уништување на личните податоци, тогаш овластеното лице за санација тоа го констатира во извештајот од ставот (2) на овој член. Извештајот се доставува до администраторот на информацискиот систем кој врз основа на извештајот, а по претходно добиено овластување од директорот на Дирекцијата, пристапува кон повторно внесување, односно враќање на личните податоци во системот.

Евиденција на инциденти

Член 7

(1) Администраторот на информацискиот систем води евиденција на инцидентите.

(2) Евиденцијата од ставот (1) на овој член ги содржи следните податоци:

- датум кога настанал инцидентот;
- име и презиме на лицето коешто го пријавило инцидентот;
- вид на инцидент;
- мерки што се преземени за санација на инцидентот;
- име и презиме на лицето коешто го санирало инцидентот;
- датум на санирање на инцидентот.

(3) При повторно внесување, односно враќање на личните податоци во системот, задолжително и во електронска форма се врши евидентирање на овластените лица коишто ја извршиле операцијата за враќање на податоците, категориите на личните податоци кои биде вратени и кои биле рачно внесени при враќањето.

(4) Евиденцијата од ставот (1) на овој член по правило се чува најмалку пет години, односно најмногу до 10 години по замена на оперативниот систем на информацискиот систем.

Влегување во сила

Член 8

Овој правилник влегува во сила на денот на неговото донесување и се објавува на веб-страната на Дирекцијата.

Директор,
Стојан Славески