Република Северна Македонија

Дирекција за безбедност
на класифицирани информации

Бр. 02- 103919

Скопје, 30 11 2021 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 член 18 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

ПОЛИТИКА
ЗА КРЕИРАЊЕ И УПОТРЕБА НА ЛОЗИНКИ ЗА АДМИНИСТРАТОРИ

Цел

Член 1

Целта на оваа политика е утврдување на начинот на креирање и употреба на лозинки за администратори на информациски систем во Дирекцијата за безбедност на класифицираните информации (во натамошниот текст: Дирекцијата).

Опсег на примена

Член 2

Оваа политика се однесува на сите корисници-администратори на информациските системи во сопственост на Дирекцијата.

Дефиниции и кратенки

Член 3

За целите на оваа политика:

- „кориснички налог“ претставува збир на права и привилегии над оперативен или информациски систем којшто, по правило, се врзува за физичко лице, а корисникот се идентификува во системот со помош на своето корисничко име и лозинка;
- „ИКТ“ значи информациски и комуникациски технологии;
- „ИКТ ресурси“ се сите сервери, мрежи, компјутери, документи, сите форми на гласовна, видео и електронска комуникација, како и комуникациските уреди во Дирекцијата за кои се води референтна листа/евиденција.

Опис

Член 4

Со оваа политика за употреба и сигурност на лозинки се дефинираат:

- типовите на лозинки,
- правила на генерирање,
- рок на важност,
- кои лозинки треба да се чуваат во писмена форма,
- место на чување,
- постапка на чување и пристап до лозинките во случај на оправдана потреба,
- постапка за замена на лозинки на кои им истекува рокот на важност,
- начин на евиденција на секој пристап кон лозинките.

Одредби за лозинки

Член 5

(1) За пристап до компјутерите, апликациите и електронските сервиси во Дирекцијата, заради спречување на неовластен пристап се отвораат кориснички налози со придружни лозинки.

(2) Лозинките што се користат за пристап до информациските системи се делат на администраторски и кориснички, при што се применуваат различни правила за нивно доделување, рок на важност, промена и чување.

(3) Зависно од можностите, потребите и проценетата ризичност на поединечни информациски системи/платформи, потребно е лозинките да се креираат на начин што ги задоволува следните минимални барања:

- да имаат определена најмала должина (на пр. 8 карактери) и
- да исполнуваат услови за комплексност на лозинката.

(4) При креирање на лозинката мора да се следат следните правила:

- да содржи големи букви (на пр. A, B, C),
- да содржи мали букви (на пр. a, b, c),
- да содржи броеви (на пр. 1, 2, 3),
- да содржи специјални знаци (на пр. #, $, &, *,?, !, -),

- да не содржи ист карактер повеќе од 2 (два) пати.

(5) Лозинката не треба да содржи поими коишто лесно се поврзуваат со корисникот (на пр. името на корисникот или зборови/изрази коишто често се користат или јасно асоцираат на корисникот, имиња на членови на семејството, имиња на домашни миленици, важни лични датуми, на пример, роденденi и слично).

(6) Администраторските налози се заклучуваат во сигурносен сеф на неопределено време, односно додека не ги отвори член од групата на систем-администратори, доколку таква група е определена.

(7) При промена на лозинката треба да се имплементира контролен механизам согласно кој нема да можат повторно да се користат одреден број на последно користени лозинки (на пр. 10).

(8) Лозинките имаат ограничен рок на важност, односно рок до кога најдоцна мораат да се променат. Рокот на важност се одредува за секој клучен ресурс посебно во Дирекцијата и може да биде најмалку 1 ден, а најмногу 30 дена.

(9) Секој корисник на лозинката е должен да иницира постапка за промена на лозинката секој пат кога постои сомневање дека неовластено лице ја дознало лозинката.

(10) Секој клучен ИКТ ресурс во Дирекцијата мора да биде конфигуриран така што ќе форсира промена на лозинката по истекот на нејзината важност.

(11) Лозинките се тајни. Секој администратор е должен да ја чува тајноста на својата лозинка и да не ја открива на други администратори.

Администраторски лозинки

Член 6

(1) Во администраторски лозинки спаѓаат лозинките на сите администраторски налози на серверите и на мрежните уреди наведени во референтната листа на клучните ИКТ ресурси/евиденцијата на Дирекцијата.

(2) Администраторските лозинки се тајни и само овластени администратори на поединечни клучни ИКТ ресурси имаат право да ги знаат. Секој од клучните ИКТ ресурси во Дирекцијата има доделен еден или повеќе администратори кои се наведени во референтната листа на клучните ИКТ ресурси/евиденцијата на Дирекцијата.

(3) Администраторските лозинки имаат ограничен рок на важност, односно рок до кога најдоцна мора да бидат променети. Рокот на важност се одредува посебно за рекој клучен ИКТ ресурс и може да биде најмалку 1 ден, а најмногу 30 дена.

(4) Освен задолжителна промена на лозинката по истекувањето на рокот на важност, секој администратор на лозинката е должен да иницира постапка за промена на лозинката секој пат кога постои сомневање дека неовластено лице ја дознало лозинката.

(5) Администраторските лозинки се чуваат во писмена форма во затворен ковert во посебен сигурносен сеф во сопственост на Дирекцијата.

(6) Раководното лице на организационата единица за ИКТ и лицето одговорно за сигурност на информациските системи се овластени за пристап до сигурносниот сеф од ставот (5) на овој член и можат да им дадат право на пристап до лозинките и на други лица. По правило, тоа можат да бидат лицата од групата на систем-администратори, доколку таква група е определена.

(7) Пристап до сигурносниот сеф овластените лица може да имаат поради редовни причини (на пр. одлагање на нови или изменети лозинки во сефот, поради истекување на рокот на важност) или поради вонредни причини (на пр. преземање на лозинки во оправдана ситуација кога лицето коешто е овластено за нивна употреба не е достапно или во ситуација на вонредна промена на лозинката за која постои сомневање дека била достапна на неовластено лице).

(8) Секој пристап кон сигурносниот сеф мора да биде во присуство на две лица од кои барем едното мора да биде овластен администратор или заменик на администраторот за соодветниот клучен ИКТ ресурс во Дирекцијата чијшто лозинка е потребна. Ова лице се потпишува во лист за евиденција во колона „Лице 1“, а другото лице посведочува на извршениот пристап со потпис во листот за евиденција во колона „Лице 2“.

(9) За секој пристап направен поради вонредни причини, лицето кое што пристапило кон сигурносниот сеф е должно да го извести лицето одговорно за сигурност на информациските системи истиот ден, а најдоцна наредниот работен ден доколку пристапот е направен надвор од работното време на Дирекцијата. Во истиот рок е потребно да се направи и вонредна промена на лозинката.

(10) При секој друг пристап кон сигурносниот сеф, лицата коишто го остварile пристапот се должни да ги запишат своите податоци во листата за евиденција на пристапот којашто се наоѓа во самиот сеф со ковертите со лозинки.

(11) Со еден пристап кон сигурносниот сеф можно е да се заменат повеќе коверти. За секој ковert се запишува датумот на остварен пристап, називот на ковертот (односно називот на серверот и на администраторскиот налог), ознака дали пристапот е редовен или вонреден тип и опис на промената.

Промена на лозинката

Член 7

Лозинките мора да се менуваат при која било од следните околности:

- најмалку еднаш на секои три месеци,
- веднаш, ако лозинката била достапна на неовластено лице или ако корисникот се сомнева дека лозинката била достапна на неовластено лице.

Примена и ревизија на политиката

Член 8

(1) Оваа политика почнува да се применува од денот на нејзиното донесување и истата се објавува на веб-страната на Дирекцијата.

(2) Оваа политика ќе се ревидира во случај на промена на основот на којшто е донесена и по потреба за изменување и дополнување на системот за заштита на личните податоци што се обработуваат во Дирекцијата.

Директор,

Стојан Славески