Врз основа на член 15 од Законот за катастар на недвижности („Службен весник на Република Македонија“ бр.55/13, 41/14, 115/14, 116/15, 153/15, 192/15, 61/16, 172/16, 64/18 и „Службен весник на Република Северна Македонија“ бр.124/19), член 18 од Статутот на Агенцијата за катастар на недвижности (бр.01-7492/10 од 30.04.2013, бр.01-548/8 од 30.01.2015година, „Службен весник на Република Македонија“бр.173/2018 и „Службен весник на Република Северна Македонија“ бр.161/20), а согласно член 18 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр.122/20), член 31 од Правилата за технички и организациски мерки за обезбедување безбедност на обработка на личните податоци во Агенцијата за катастар на недвижности бр. 0204-12219/1 од 24.08.2021 година и согласно член 8 од Политиката за создавање на систем за заштита на лични податоци во Агенцијата за катастар на недвижности бр.0204-12218/1 од 24.08.2021 година, директорот на Агенцијата за катастар на недвижности донесе

ПОЛИТИКА ЗА КРЕИРАЊЕ И УПОТРЕБА НА ЛОЗИНКИ ЗА АДМИНИСТРАТОРИ

Целта на овој документ е формално да дефинира политика во организацијата која се однесува на креирање и употреба на лозинки за администратори.

1. Област на примена

Политиката за креирање и употреба на лозинки за администратори (понатаму Политиката) се однесува на сите корисници-администратори на информацискиските системи на Агенцијата за катастар на недвижности.

2. Дефиниции, ознаки и кратенки

Кориснички налог – множество на права и привилегии над оперативен или информациски систем. По правило корисничкиот налог се врзува за физичко лице. Корисникот се идентификува во системот со помош на своето корисничко име и лозинка.

ИКТ ресурси – ги вклучуваат сите сервери, мрежи, компјутери, документи, како и сите форми на гласовна, видео и електронска комуникација, и комуникациски уреди во организацијата.

3. Опис

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

- типовите на лозинки
- правила на генерирање
- век на траење
- 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 на замена на лозинки на кои им истекува рокот на траење
- начин на евиденција на секој пристап кон лозинките

4. Одредби за лозинки

За пристап кон компјутерите, апликациите и електронските сервиси во организацијата, заради спречување на неовластен пристап се отвораат кориснички налози со придружни лозинки.

Лозинките кои се користат за пристап кон информациските системи се делат на администраторски и кориснички, при што се применуваат различни правила за нивно доделување, век на траење, промена и чување.

Зависно од можностите, потребите и проценетата ризичност на поединечни информациски системи/платформи, потребно е лозинките да се креираат така што да ги задоволат следните минимални барања:

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

Лозинката мора да исполнува најмалку три од следните четири правила и тоа да содржи:

- големи букви(на пример:A,B,C)
- мали букви(на пример:a,b,c)
- броеви(на пример:0,1,2)
- специјални знаци(#,&,!,%,|,?,-,*)
- ист знак не смее да се појавува повеќе од 2 (два) пати

- да не содржи поими кои лесно се поврзуваат со корисникот (името на корисникот или зборови/изрази кои често се користат или кои лесно асоцираат на корисникот, имиња на членови од семејството, имиња на домашни миленици,родендени...)

- администраторските налози се заклучуваат на неопределено време, односно додека не ги ослободи член на администраторската група)

- да се имплементира контрола при промена на лозинката да не можат повторно да се користат одреден број последно користени лозинки (10)

Лозинките имаат ограничен век на траење, односно рок до кога најдоцна мораат да се променат. Векот на траење се одредува за секој клучен ресурс во организацијата посебно, и може да биде најмалку 1 ден, а најмногу 30 денови. Секој клучен ИТ/ИС ресурс во организацијата мора да биде конфигуриран така што ќе форсира промена на лозинката по истекот на нејзиното траење.

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

5. Администраторски лозинки

Во администраторски лозинки спаѓаат лозинките на сите администраторски налози на серверите односно мрежните уреди наведени во Референтната листа на клучните информациски ресурси на организацијата.

Администраторските лозинки се тајни, и само овластени администратори на поединечните клучни ресурси имаат право да ги знаат. Секој од клучните компјутерски ресурси во организацијата има доделен еден или повеќе администратори кои се наведени во Референтната листа на компјутерски администратори во организацијата.

Администраторските лозинки имаат ограничен век на траење, односно рок до кога најдоцна мора да бидат променети. Векот на траење се одредува посебно за секој клучен информациски ресурс на организацијата, и може да биде најмалку 1 ден а најмногу 30 дена. Освен задолжителната промена на лозинката по истекувањето на рокот на траење, секој администратор, односно корисник на лозинка е должен да иницира постапка за промена на лозинката секој пат кога постои сомневање дека неовластено лице ја дознало лозинката.

Администраторските лозинки се чуваат во писмена форма во пликови во посебен сигурносен сеф кој гласи на организацијата и се користи исклучително за таа намена. Раководителот на Сектор за информатички и комуникациски технологии и Лицето одговорно за сигурност на информациските системи се овластени личности кои имаат пристап кон сефот. Раководителот на Сектор за информатички и комуникациски технологии и Лицето одговорно за сигурност на информациските системи можат да им дадат право на пристап кон лозинките и на други лица. По правило, ова можат да бидат лицата од групата на систем администратори.

На сигурносниот сеф, овластените лица можат да му пристапуваат поради редовни причини (одлагање на нови или изменети лозинки во сефот, поради истекување на рокот на траење) или поради вонредни причини (преземање на лозинки во оправдано потребна ситуација, а личноста која е овластена за нивна употреба не е

достапна, и во ситуација на вонредна промена на лозинката за која постои сомневање дека е достапна на неовластени лица).

Секој пристап кон сигурносниот сеф мора да го направат две лица, од кои барем едно мора да биде овластен администратор или заменик на администраторот за соодветниот клучен информациски ресурс на организацијата чија лозинка е потребна. Ова лице се потпишува во лист за евиденција во колона "Лице 1". Другото лице посведочува на извршениот пристап со потпис во лист за евиденција во колона "Лице 2".

За секој пристап направен поради вонредни причини, лицето кое пристапило кон сигурносниот сеф должно е да го извести Лицето одговорно за сигурност на информациските системи истиот ден, односно најдоцна следниот работен ден, ако пристапот е направен надвор од работното време на организацијата. Во истиот рок е потребно да се направи и вонредна промена на лозинката.

При секој друг пристап кон сигурносниот сеф, лицата кои пристапиле се должни да ги запишат своите податоци во листата за евиденција на пристапот која се наоѓа во самиот сигурносен сеф со пликовите за лозинки. Со еден пристап кон сигурносниот сеф можно е да се заменат повеќе пликови, а за секој плик се запишува датумот на пристап, називот на пликот (односно називот на серверот и администраторскиот налог), ознака дали пристапот е од редовен или вонреден тип и опис на промената.

6.Промена на лозинка

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

- Најмалку еднаш на секои три месеци
- Веднаш, ако лозинката е искомпромитирана или ако корисникот се сомнева дека е компромитирана

7. Објава

Оваа политика влегува во сила со денот на донесувањето и истата се објавува на ВЕБ страницата на АКН .

ДИРЕКТОР

м-р Борис Тунцев