ს ა ქ ა რ თ ვ ე ლ ო
სენაკის მუნიციპალიტეტის მერი

ბრძანება:**ბ40.40221452**

თარიღი:**25/05/2022**

პაროლების მართვის წესის დამტკიცების შესახებ

საქართველოს ორგანული კანონის „ადგილობრივი თვითმმართველობის კოდექსი“ 54-ე მუხლის პირველი პუნქტის ,,ე. ე.” ქვეპუნქტის, 61-ე მუხლის მე-3 პუნქტის ,,ა” ქვეპუნქტის და საქართველოს კანონის „საქართველოს ზოგადი ადმინისტრაციული კოდექსი“ 52-ე მუხლის საფუძველზე

ვ ბ რ ძ ა ნ ე ბ :

1. დამტკიცდეს პაროლების მართვის წესი თანდართული დანართი №1-ის შესაბამისად.

2. კონტროლს ბრძანების შესრულებაზე განვახორციელებ პირადად.

3. ბრძანება ძალაშია გაცნობისთანავე.

4. ბრძანება შეიძლება გასაჩივრდეს გაცნობიდან ერთი თვის ვადაში სენაკის რაიონულ სასამართლოში (მის: ქ. სენაკი, შ. რუსთაველის ქ. №247).

ვახტანგ გადელია

სენაკის მუნიციპალიტეტის მერია-მერი

გამოყენებულია კვალიფიციური
ელექტრონული ხელმოწერა/
ელექტრონული შტამპი

ქ. სენაკი, 4100, ი.ჭავჭავაძის.№103 ტელ.: (0 413) 27 75 47
ელ-ფოსტა: SENAKISMERIA@GMAIL.COM ვებ: WWW.SENAKI.GOV.GE

დანართი №1

პაროლების მართვის წესი

მუხლი 1. ზოგადი დებულებები

1. დოკუმენტის მიზანია სენაკის მუნიციპალიტეტის მერიის (შემდგომში - მერია) მიერ დამუშავებულ მონაცემებზე არაავტორიზებული წვდომის შეზღუდვის გზით პერსონალურ მონაცემთა უსაფრთხოებისათვის სათანადო ორგანიზაციული და ტექნიკური ზომების მიღება და მერიის მიერ გამოყენებულ კომპიუტერებზე, ქსელებსა და სისტემებზე პაროლების მართვისა და უსაფრთხო გამოყენების წესების განსაზღვრა.

2. ამ წესის მოქმედება ვრცელდება მერიაში დასაქმებულ ყველა პირზე, რომელიც სარგებლობს მერიის კომპიუტერით და/ან ელექტრონული სისტემით და, ასევე, მერიის მიზნებით გამოყენებულ ნებისმიერ ელექტრონულ სისტემაზე მიუხედავად მისი მფლობელისა, ფორმისა და სხვა მახასიათებლებისა.

მუხლი 2. მომხმარებლის შექმნა

1. კომპიუტერსა და ელექტრონულ სისტემაში შესასვლელად თითოეულ დასაქმებულს ენიჭება მომხმარებლის სახელი და პაროლი. პაროლი თანამშრომლის მიერ უნდა განისაზღვროს ინდივიდუალურად და კონფიდენციალურად.

2. მერიაში ახალი თანამშრომლის დანიშვნისას, მისი დანიშვნის ბრძანებას ადამიანური რესურსების მართვის განყოფილება უგზავნის სსიპ მუნიციპალური სერვისების განვითარების სააგენტოს, რომელიც ქმნის შესაბამისი თანამშრომლის მომხმარებლის სახელს და პირველად პაროლს, თანამშრომლის სამუშაო აღწერილობიდან გამომდინარე განსაზღვრავს სისტემაში მის უფლებებს (რა ტიპის ხედვა/წვდომა აქვს მომხმარებელს).

3. მომხმარებლის შექმნის შემდეგ, მისი საბოლოო აქტივაციისათვის, ქმედებას ეთანხმება (ავიზებს) მერი.

4. ხოლო თანამშრომელზე ტექნიკის გაპიროვნების შემთხვევაში აი ტი სპეციალისტი ქმნის შესაბამისი თანამშრომლის მომხმარებლის სახელს და პირველად პაროლს.

მუხლი 3. პაროლების მართვა და უსაფრთხო გამოყენება

1. მერია ადგენს პაროლების დაყენების, განახლებისა და მათთან მოპყრობის წესებსა და სტანდარტებს და უზრუნველყოფს ამ წესების შესრულებას.

2. აი ტი სპეციალისტი უზრუნველყოფს პაროლების დაშიფრული სახით, უსაფრთხოდ და განცალკევებით შენახვას.

3. მერიაში პაროლები გამოიყენება ნებისმიერი კომპიუტერისა და ელექტრონული სისტემის მიმართ, რომლის საშუალებითაც მუშავდება/შეიძლება მუშავდებოდეს პერსონალური მონაცემები.

4. მერიაში მოქმედებს შემდეგი პრინციპები:

ა) თითოეული მომხმარებელი იყენებს მხოლოდ საკუთარ/ინდივიდუალურ მომხმარებლის სახელსა და პაროლს;

ბ) თითოეული მომხმარებელი წერილობით, მათ შორის, ამ დოკუმენტის გაცნობის გზით, არის ინფორმირებული/გაფრთხილებული პაროლის საიდუმლოდ შენახვისა და გაუმჟღავნებლობის მნიშვნელობისა და ვალდებულების შესახებ;

გ) პირველადი/დროებითი პაროლების გამოყენება დასაშვები მხოლოდ სისტემაში პირველად შესვლის დროს (first log-on) და მომხმარებელი ვალდებულია შეცვალოს ის;

დ) პირველადი/დროებითი პაროლები მომხმარებლებს მიეწოდება ინდივიდუალურად, უსაფრთხო გზის/არხის გამოყენებით;

ე) გამოყენებული პაროლები უნდა იყოს რთული და სისტემა ითხოვდეს მის ცვლილებას მინიმუმ ყოველ 3 თვეში;

მუხლი 4. ვალდებულებები

1. თანამშრომელი ვალდებულია დაიცვას პაროლის საიდუმლოება და არ გახადოს ის ხელმისაწვდომი მესამე პირებისთვის, მათ შორის, სხვა თანამშრომლებისთვის, აი ტი პერსონალისთვის, უშუალო უფროსისათვის და ა. შ. მომხმარებლის სახელისა და პაროლის შესახებ ინფორმაციის სხვა პირისათვის (მათ შორის სხვა თანამშრომლისათვის) გადაცემის შემთხვევაში შესაძლოა გამოყენებულ იქნეს დისციპლინური პასუხისმგებლობის ზომა.

2. თანამშრომელმა პაროლები არ უნდა შეინახოს სხვისთვის ხელმისაწვდომ ადგილას (მაგ. სამუშაო მაგიდაზე რომელიმე ფურცელზე, კომპიუტერის დესკტოპზე, კლავიატურის ქვეშ და ა. შ.)

3. თანამშრომელმა არ უნდა აირჩიოს სისტემის მიერ პაროლის დამახსოვრების ფუნქცია.

4. თანამშრომელმა უნდა შეცვალოს პაროლი სისტემაში პირველად შესვლისას, სისტემის მოთხოვნის შემთხვევაში პერიოდულად და მაშინვე, თუ ეჭვი გაუჩნდა მის კომპრომეტაციაზე.

5. თანამშრომელმა არ უნდა გამოიყენოს მარტივი და/ან ერთი და იგივე პაროლი რამდენიმე სისტემაზე.

6. რეკომენდებულია თანამშრომელმა პაროლად არ გამოიყენოს მარტივი კომბინაციები, არსებული ლექსიკური სიტყვები/სიტყვათშეთანხმებები და ა. შ. (მაგ.: 123; Password, Enterpassword, Senaki.gov).

7. თანამშრომელს ეკრძალება სხვისი პაროლების მოპოვება, სხვის კომპიუტერთან და/ან მონაცემებთან არაავტორიზებული წვდომა.