დანართი №1

პაროლების მართვის წესი

მუხლი 1. ზოგადი დებულებები

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

2. ამ წესის მოქმედება ვრცელდება საკრებულოში დასაქმებულ ყველა პირზე, რომელიც სარგებლობს საკრებულოს კომპიუტერით და/ან ელექტრონული სისტემით და, ასევე, საკრებულოს 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. საკრებულოში 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) საკრებულოს თავმჯდომარე.

4. ხოლო თანამშრომელზე ტექნიკის გაპიროვნების შემთხვევაში **აი-ტი** (IT) სპეციალისტი ქმნის შესაბამისი თანამშრომლის მომხმარებლის სახელს და პირველად პაროლს.

მუხლი 3. პაროლების მართვა და უსაფრთხო გამოყენება

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

2. აი-ტი (IT) სპეციალისტი უზრუნველყოფს პაროლების დაშიფრული სახით, უსაფრთხოდ და განცალკევებით შენახვას.

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

4. საკრებულოში 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;

მუხლი 4. ვალდებულებები

1. თანამშრომელი ვალდებულია დაიცვას პაროლის საიდუმლოება და არ გახადოს ის ხელმისაწვდომი მესამე პირებისთვის, მათ შორის, სხვა თანამშრომლებისთვის, **აი-ტი (IT)** 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, NoNo).

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