

# ციფრული მმართველობის სააგენტოს თავმჯდომარის

## ბრძანება №6

2020 წლის 16 ოქტომბერი

ქ. თბილისი

### ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის დამტკიცების შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-11 მუხლის მე-2 პუნქტის „ვ“ ქვეპუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის, მე-13 მუხლის პირველი და მე-7 პუნქტებისა და „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის 25-ე მუხლის შესაბამისად, ვბრძანებ:

#### მუხლი 1

დამტკიცდეს „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი“.

#### მუხლი 2

ძალადაკარგულად გამოცხადდეს „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის №1 ბრძანება.

#### მუხლი 3

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

სსიპ ციფრული მმართველობის  
სააგენტოს თავმჯდომარე

გიორგი მეულუმიანი

### ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი

#### მუხლი 1. ინფორმაციული უსაფრთხოების აუდიტის მიზანი, გავრცელების სფერო

1. ინფორმაციული უსაფრთხოების აუდიტის მიზანია კრიტიკული ინფორმაციული სისტემის სუბიექტის (შემდგომ – ორგანიზაცია) ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების – ინფორმაციული უსაფრთხოების პოლიტიკის საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს (შემდგომ – სააგენტო) მიერ დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შეფასება გარე აუდიტის (შემდგომ – აუდიტის) საშუალებით, რის საფუძველზეც დგება დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა.

2. ინფორმაციული უსაფრთხოების აუდიტის ჩატარება ხდება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით გათვალისწინებული წესით იმ ორგანიზაციებში, რომლებიც ამავე კანონის მე-11 მუხლის პირველი პუნქტის თანახმად იდენტიფიცირებულნი არიან, როგორც კრიტიკული ინფორმაციული სისტემის სუბიექტები.

#### მუხლი 2. აუდიტის ჩატარების უფლებამოსილების მქონე პირები

1. ორგანიზაციაში აუდიტის ჩატარების უფლება აქვთ მხოლოდ იმ პირებს, რომლებიც „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონისა და „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესის, ავტორიზაციის პროცედურებისა და ავტორიზაციის საფასურის დამტკიცების შესახებ“ სააგენტოს თავმჯდომარის ბრძანების შესაბამისად, სათანადო ავტორიზაციას გაივლიან სააგენტოში.

2. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-6 მუხლის პირველი პუნქტის



თანხმად, აუდიტის ჩატარების უფლებამოსილება აქვს ასევე სააგენტოს.

3. სააგენტოს მიერ ჩატარებული აუდიტის საფასური განისაზღვრება „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს მიერ მომსახურების გაწევის საფასურების განაკვეთების, საფასურების გადახდის, მათი გადახდისგან გათავისუფლებისა და გადახდილი საფასურების დაბრუნების წესის დამტკიცების შესახებ“ საქართველოს მთავრობის 2020 წლის 13 ივლისის №438 დადგენილებით.

### **მუხლი 3. აუდიტის ჩატარების პრინციპები**

1. აუდიტი უნდა ჩატარდეს ყოველწლიურად. მისი ჩატარების გადავადება შესაძლებელია, მხოლოდ მნიშვნელოვანი არგუმენტების არსებობის შემთხვევაში, 6 თვით, ციფრული მმართველობის სააგენტოსთან შეთანხმების საფუძველზე.

2. აუდიტის ჩატარებისას დაცული უნდა იქნეს შემდეგი პრინციპები:

ა) საქმის კეთილსინდისიერად და პასუხისმგებლობით შესრულება;

ბ) მიუკერძოებლობა;

გ) აუდიტის პროცესში მოსალოდნელი გავლენებისადმი სიმტკიცის გამოჩენა;

დ) სამართლიანობა (ზუსტი და ჭეშმარიტი ანგარიშების ვალდებულება);

ე) აუდიტის ჩატარებისას სათანადო ყურადღება;

ვ) კონფიდენციალურობა (ინფორმაციის უსაფრთხოება);

ზ) დამოუკიდებლობა (აუდიტის მიუკერძოებლობისა და აუდიტის დასკვნების ობიექტურობის საფუძველი);

თ) მტკიცებულებებზე ორიენტირებული მიდგომა: აუდიტის სანდო და განმეორებადი დასკვნების მიღების გონივრული მეთოდი.

### **მუხლი 4. აუდიტის ანგარიში**

1. ორგანიზაციამ აუდიტის ჩატარების შესახებ ანგარიში უნდა წარუდგინოს ციფრული მმართველობის სააგენტოს აუდიტის დასრულებიდან 10 სამუშაო დღის განმავლობაში.

2. ანგარიში უნდა მოიცავდეს შემდეგ საკითხებს:

ა) აუდიტის მიზნებს;

ბ) აუდიტის გავრცელების სფეროს;

გ) აუდიტის გუნდის და აუდიტს დაქვემდებარებული ორგანიზაციის მონაწილეებს;

დ) აუდიტის აქტივობების ჩატარების ადგილმდებარეობას, თარიღსა და დროს;

ე) აუდიტის კრიტერიუმებს;

ვ) აუდიტის აღმოჩენებსა და მათთან დაკავშირებულ მტკიცებულებებს;

ზ) აუდიტის დასკვნებს;

თ) აუდიტის კრიტერიუმების შესრულების მდგომარეობას.



3. აუდიტის ანგარიში უნდა იყოს დათარიღებული, განხილული და დამტკიცებული.

## **მუხლი 5. აუდიტის შემდგომი ქმედებები**

1. აუდიტის მიზნებიდან გამომდინარე, აუდიტის დასკვნები შესაძლოა მიუთითებდეს ინფორმაციული უსაფრთხოების მართვის სისტემაში გარკვეულ შესწორებებზე, მაკორექტირებელ, პრევენციულ ან გაუმჯობესების აქტივობებზე.

2. ინფორმაციული უსაფრთხოების მართვის სისტემაში ცვლილებების და სამოქმედო გეგმის განახლების შესახებ გადაწყვეტილებას იღებს ორგანიზაცია.

3. თუ აუდიტის ჩატარების შედეგად გამოვლინდა ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნებთან შეუსაბამობა, ორგანიზაცია იკვლევს შეუსაბამობის მიზეზებს და, საჭიროების შემთხვევაში, განსაზღვრავს და ახორციელებს სათანადო გამოსასწორებელ ღონისძიებებს, რომელთა გრაფიკსაც წარუდგენს სააგენტოს.

