მონაცემთა გაცვლის სააგენტოს თავმჯდომარის

ბრძანება №1

2013 წლის 4 თებერვალი

ქ. თბილისი

ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის დამტკიცების შესახებ

,,საჯარო სამართლის იურიდიული პირის - მონაცემთა გაცვლის სააგენტოს შექმნის შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის ბ[1] ქვეპუნქტისა და ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-11 მუხლის მე-2 პუნქტის ,,ვ“ ქვეპუნქტის თანახმად, **ვბრძანებ:**

მუხლი 1

დამტკიცდეს „აუდიტის ჩატარების წესი”.

მუხლი 2

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

მონაცემთა გაცვლის სააგენტოს
თავმჯდომარე **ირაკლი გვენეტაძე**

ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი

მუხლი 1. ინფორმაციული უსაფრთხოების აუდიტის მიზანი, გავრცელების სფერო

1. ინფორმაციული უსაფრთხოების აუდიტის მიზანია კრიტიკული ინფორმაციული სისტემის სუბიექტის (შემდგომში - ,,ორგანიზაციის“) ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების - ინფორმაციული უსაფრთხოების პოლიტიკის მონაცემთა გაცვლის სააგენტოს მიერ დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შეფასება გარე აუდიტის (შემდგომში - 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 აქვს 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 მონაცემთა გაცვლის სააგენტოს ბრძანების შესაბამისად სათანადო ავტორიზაციას გაივლიან მონაცემთა გაცვლის სააგენტოში.

2. ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-6 მუხლის პირველი პუნქტის თანახმად, აუდიტის ჩატარების უფლებამოსილება აქვს ასევე მონაცემთა გაცვლის სააგენტოს.

3. მონაცემთა გაცვლის სააგენტოს მიერ ჩატარებული აუდიტის საფასური განისაზღვრება კრიტიკული ინფორმაციული სისტემის სუბიექტთან გაფორმებული ხელშეკრულებით.

მუხლი 3. აუდიტის ჩატარების პრინციპები

1. აუდიტი უნდა ჩატარდეს ყოველწლიურად. მისი ჩატარების გადავადება შესაძლებელია მხოლოდ მნიშვნელოვანი არგუმენტების არსებობის შემთხვევაში, ნახევარი წლით, მონაცემთა გაცვლის სააგენტოსთან შეთანხმების საფუძველზე.

2. აუდიტის ჩატარებისას გასათვალისწინებელია მთელი რიგი პრინციპების დაცვა:

ა) საქმის კეთილსინდისიერად და პასუხისმგებლობით შესრულება;

ბ) მიუკერძოებლობა;

გ) აუდიტის პროცესში მოსალოდნელი გავლენებისადმი სიმტკიცის გამოჩენა;

დ) სამართლიანობა: ზუსტი და ჭეშმარიტი ანგარიშგების 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 ჩატერების შესახებ ანგარიში უნდა წარუდგინოს მონაცემთა გაცვლის სააგენტოს აუდიტის დასრულებიდან 10 სამუშაო დღის განმავლობაში.
2. ანგარიში უნდა მოიცავდეს შემდეგ საკითხებს:
ა) აუდიტის მიზნები;
ბ) აუდიტის გავრცელების სფერო;
გ) აუდიტის გუნდის და აუდიტს დაქვემდებარებული ორგანიზაციის მონაწილეები;
დ) აუდიტის აქტივობების ჩატარების ადგილმდებარეობა, თარიღი და დრო;
ე) აუდიტის კრიტერიუმები;
ვ) აუდიტის აღმოჩენები და მათთან დაკავშირებული მტკიცებულებები;
ზ) აუდიტის დასკვნები;
თ) აუდიტის კრიტერიუმების შესრულების მდგომარეობა.
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 მონაცემთა გაცვლის სააგენტოს.