მონაცემთა გაცვლის სააგენტოს თავმჯდომარის

ბრძანება №6

2013 წლის 4 თებერვალი

ქ. თბილისი

ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესის, ავტორიზაციის პროცედურები და ავტორიზაციის საფასურის 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 ,,ე“ ქვეპუნქტის თანახმად, **ვბრძანებ**

მუხლი 1

დამტკიცდეს “ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესი, ავტორიზაციის პროცედურები და ავტორიზაციის საფასური”.

მუხლი 2

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

მონაცემთა გაცვლის სააგენტოს
თავმჯდომარე **ირაკლი გვენეტაძე**

ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესი, ავტორიზაციის პროცედურები და ავტორიზაციის საფასური

მუხლი 1. ინფორმაციული უსაფრთხოების აუდიტის მიზანი, გავრცელების სფერო

1. ინფორმაციული უსაფრთხოების აუდიტის მიზანია კრიტიკული ინფორმაციული სისტემის სუბიექტის (შემდგომში – ორგანიზაცია) ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების – ინფორმაციული უსაფრთხოების პოლიტიკის საჯარო სამართლის იურიდიული პირის – მონაცემთა გაცვლის სააგენტოს (შემდგომში –სააგენტო) მიერ დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შეფასება, რის საფუძველზეც დგება დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა.

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

მუხლი 2. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირები

1. ორგანიზაციაში ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლება აქვს მხოლოდ იმ პირებს, რომლებიც ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონისა და ამ წესის შესაბამისად სათანადო ავტორიზაციას გაივლიან სააგენტოში (შემდგომში - ავტორიზებული აუდიტორული ორგანიზაცია).

2. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი განსაზღვრულია ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონითა და ,,ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანებით.

მუხლი 3. ავტორიზაციის შინაარსი, მიზანი

1. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფებამოსილების მქონე პირთა ავტორიზაციის მიზანია შესაბამისი საქმიანობის განხორციელებისათვის აუცილებელი სტანდარტების (წესების)

დაკმაყოფილების უზრუნველყოფა.
2. სტანდარტი (წესები) არის სახელმწიფოს (სააგენტოს) მიერ დაწესებული მოთხოვნა, რომელსაც უნდა აკმაყოფილებდეს აპლიკანტი ორგანიზაცია იმისათვის, რომ ჩაატაროს ინფორმაციული უსაფრთოების აუდიტი „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონისა და ამ ბრძანების შესაბამისად.
3. ავტორიზაცია არის აპლიკანტი ორგანიზაციის დადგენილ წესებთან შესაბამისობის გარე შეფასების მექანიზმი, რომელსაც ახორციელებს სააგენტო.
4. აპლიკანტი ორგანიზაციის მიერ ავტორიზაციისას წარმოდგენილი აუდიტორები ავტორიზაციის გავლის შემდეგ ავტომატურად ითვლებიან ინფორმაციული აუდიტის ჩატარებაზე ავტორიზებულ პირებად.

მუხლი 4. ავტორიზაციის გავლის წესი

ავტორიზაციის გავლის უფლება აქვს საქართველოში რეგისტრირებულ ნებისმიერ იურიდიულ პირს, რომელიც ფლობს კვალიფიციურ კადრს და სარგებლობს სანდოობის მაღალი ხარისხით და წარმატებული საქმიანი რეპუტაციით.

მუხლი 5. ავტორიზაციისათვის წარსადგენი დოკუმენტები
1. აპლიკანტი ორგანიზაცია მისი უფლებამოსილი წარმომადგენლის მეშვეობით ავსებს თანდართულ განაცხადის ფორმას (დანართი 1).
2. განაცხადთან ერთად აპლიკანტი ორგანიზაცია სააგენტოში ასევე წარადგენს:
ა) აპლიკანტ ორგანიზაციაში დასაქმებული აუდიტორების შესახებ ინფორმაციას, რომლებიც ჩაატარებენ ინფორმაციული უსაფრთხოების აუდიტს;
ბ) ინფორმაციული უსაფრთხოების აუდიტორთა CV-ებს;
გ) აპლიკანტ ორგანიზაციასთან დასაქმებულ ინფორმაციული უსაფრთხოების აუდიტორთა კომპეტენციის დამადასტურებელ ცნობებს - მოქმედ სერტიფიკატებს/დიპლომებს ინფორმაციული უსაფრთხოების აუდიტის მიმართულებით „ISMS Lead Audit Certificate“, რომელიც აღიარებულია The International Register of Certificated Auditors (IRCA)-ს მიერ ან Information Systems Audit and Control Association-ის მიერ გაცემული CISA Certificate;
დ) აპლიკანტი ორგანიზაციის უფლებამოსილი პირის განაცხადი/თანხმობა იმის თაობაზე, რომ ინფორმაციული უსაფრთხოების აუდიტის ჩატარებისას მის მიერ დაცული იქნება დამოუკიდებლობის, კონფიდენციალურობის, ობიექტურობის და მიუკერძოებლობის პრინციპები.
3. აპლიკანტი ორგანიზაცია დოკუმენტაციას წერილობით აგზავნის სააგენტოში.

მუხლი 6. ავტორიზაციის პროცედურები
1. სააგენტო ამოწმებს შემოსული დოკუმენტაციის შესაბამისობასა და სისრულეს, ხოლო თუ აპლიკანტი ორგანიზაციის მიერ არ არის სრულად წარმოდგენილი ყველა დოკუმენტაცია, საბუთების მიღებიდან 5 სამუშაო დღის ვადაში ატყობინებს მას აღნიშნულის შესახებ წერილობით და აძლევს დამატებით ვადას ხარვეზის შესავსებად.
2. სააგენტო იტოვებს უფლებას, შეკითხვების არსებობის შემთხვევაში, აპლიკანტ ორგანიზაციას მოსთხოვოს დამატებითი ინფორმაციის წარდგენა ან/და დაზუსტება.
3. აპლიკანტი ორგანიზაციის მიერ დადგენილ ვადაში დამატებით მოთხოვნილი დოკუმენტების წარუდგენლობის შემთხვევაში, სააგენტო იტოვებს უფლებას, უარი უთხრას მას ავტორიზაციის გავლაზე.

მუხლი 7. ავტორიზაციის შესახებ გადაწყვეტილების მიღების პროცედურები
1. ავტორიზაციის შესახებ გადაწყვეტილებას იღებს სააგენტო.
2. ავტორიზაციის შესახებ გადაწყვეტილება მიიღება კოლეგიური წესით, რისთვისაც სააგენტოს თავმჯდომარე ქმნის სამუშაო ჯგუფს 4 თანამშრომლის შემადგენლობით, რომელსაც თავად ხელმძღვანელობს.
3. უსაფრთხოების შემოწმების მიზნით სააგენტო უფლებამოსილია კონსულტაციები გაიაროს შესაბამისი უწყებების წარმომადგენლებთან.
4. სამუშაო ჯგუფის წევრსა და აპლიკანტ ორგანიზაციას შორის ინტერესთა კონფლიქტის არსებობის შემთხვევაში, სამუშაო ჯგუფის წევრი ვალდებულია განაცხადოს აღნიშნულის შესახებ, ხოლო თავმჯდომარე ვალდებულია დანიშნოს სამუშაო ჯგუფის ახალი წევრი.
5. სამუშაო ჯგუფის თითოეული წევრი ყოველი ახალი განაცხადის განხილვამდე ხელს აწერს ინტერესთა კონფლიქტის არარსებობის შესახებ განცხადებას.
6. სამუშაო ჯგუფი გადაწყვეტილებას იღებს ხმათა უმრავლესობით.

მუხლი 8. ავტორიზაციის მოთხოვნები
1. აპლიკანტი ორგანიზაციის მიერ სარეგისტრაციოდ წარმოდგენილი აუდიტორი/აუდიტორები ინფორმაციული უსაფრთხოების აუდიტს უნდა ახორციელებდეს მხოლოდ ამ აპლიკანტი ორგანიზაციის სახელით.

2. აპლიკანტ ორგანიზაციას უნდა ჰყავდეს სულ მცირე ერთი აუდიტორი, რომელიც რეგისტრაციის მომენტში სერტიფიცირებული იქნება British Standard Institute-ის, International Standard Organization-ის ან Information Systems Audit and Control Association-ის მიერ ინფორმაციულ უსაფრთხოებაში.
3. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლება აქვთ მხოლოდ ავტორიზებული აუდიტორული ორგანიზაციების ავტორიზებულ აუდიტორებს აუდიტის პერიოდში მოქმედი სერტიფიკატებით.
4. ავტორიზაციისას უზრუნველყოფილი უნდა იყოს დამოუკიდებლობის, კონფიდენციალურობის, ობიექტურობის და მიუკერძოებლობის პრინციპების დაცვა.

მუხლი 9. ავტორიზაციის შესახებ გადაწყვეტილების მიღება

1. სააგენტო ამოწმებს აპლიკანტი ორგანიზაციის მიერ წარდგენილ დოკუმენტაციას და ავტორიზაციის მიცემის შესახებ გადაწყვეტილებას იღებს შემდეგი კრიტერიუმების გათვალისწინებით:
ა) აპლიკანტი ორგანიზაციის ინფორმაციული უსაფრთხოების აუდიტორის კომპეტენცია, რომელიც მოწმდება წარმოდგენილი სერტიფიკატების და სამუშაო გამოცდილების გათვალისწინებით;
ბ) აპლიკანტი ორგანიზაციის ინფორმაციული უსაფრთხოების აუდიტორის უსაფრთხოების შემოწმების გავლით;
2. სააგენტო გადაწყვეტილებას იღებს დოკუმენტაციის სრულად წარდგენიდან 90 კალენდარული დღის განმავლობაში.
3. აპლიკანტ ორგანიზაციას პასუხი წერილობით ეცნობება.
4. დადებითი პასუხის შემთხვევაში აპლიკანტ ორგანიზაციას ეცნობება მის მიერ წარმოდგენილი აუდიტორებიდან რომელმა დააკმაყოფილა ავტორიზაციის მოთხოვნები.
5. დადებითი პასუხის შემთხვევაში აპლიკანტ ორგანიზაციაზე გაიცემა ავტორიზაციის შესაბამისი სერტიფიკატი უნიკალური ნომრით. აპლიკანტ ორგანიზაციას ავტორიზაცია ეძლევა 3 წლის ვადით (ავტორიზაციის პერიოდი).
6. ყოველწლიურად ავტორიზებულმა აუდიტორულმა ორგანიზაციამ უნდა ჩაატაროს შუალედური თვითშეფასება ავტორიზაციის მოთხოვნებთან შესაბამისობის შემოწმების მიზნით.
7. ავტორიზაცია ავტომატურად უქმდება, თუ:
ა) ავტორიზებული აუდიტორებიდან არცერთი აღარ მუშაობს მოცემულ ავტორიზებულ აუდიტორულ ორგანიზაციაში;
ბ) გაცემული სერტიფიკატი არის ძალადაკარგული აუდიტორის მიერ ინფორმაციული უსაფრთხოების აუდიტის ჩატარებისას;
8. ავტორიზებული აუდიტორული ორგანიზაცია, თუ მან დაკარგა ავტორიზაცია ზემოაღნიშნული საფუძვლით, ვალდებულია ხელახლა გაიაროს ავტორიზაციის პროცედურა, იმისათვის რომ მოიპოვოს ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლება.
9. ავტორიზებული აუდიტორული ორგანიზაციის ინფორმაციული უსაფრთხოების აუდიტორის/აუდიტორთა სხვა დაწესებულებაში გადასვლა არ იწვევს ამ უკანასკნელის მიერ ავტორიზაციის ავტომატურად მოპოვებას. აღნიშნულმა დაწესებულებამ უნდა გაიაროს ავტორიზაციის პროცედურა მოცემული წესების შესაბამისად, იმისათვის რომ მოიპოვოს ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლება.

მუხლი 10. ავტორიზებულ აუდიტორულ ორგანიზაციაში ახალი აუდიტორის რეგისტრაცია

1. იმ შემთხვევაში, თუ ავტორიზებული აუდიტორული ორგანიზაცია მიიღებს გადაწყვეტილებას აიყვანოს ახალი აუდიტორი ინფორმაციული უსაფრთხოების სფეროში, მას ევალება სააგენტოში წარმოადგინოს განაცხადი (დანართი 1) და ამ წესის მე-5 მუხლით მოთხოვნილი დოკუმენტაცია.
2. აღნიშნულ შემთხვევაში გადაწყვეტილება მიიღება ამ წესის მე-9 მუხლით დადგენილი წესით.

მუხლი 11. ავტორიზებული აუდიტორული ორგანიზაციების კატალოგი

1. სააგენტო საჯაროდ ხელმისაწვდომს ხდის მის მიერ ავტორიზებული აუდიტორული ორგანიზაციებისა და აუდიტორების კატალოგს.
2. ავტორიზირებული აუდიტორული ორგანიზაციები და აუდიტორები წინასწარ აძლევენ თანხმობას სააგენტოს მათ მიერ წარმოდგენილი მონაცემების კატალოგში განთავსებისა და ამგვარად, საჯაროდ ხელმისაწვდომობის შესახებ.
3. კატალოგში განთავსდება შემდეგი მონაცემები:
ა) ავტორიზებული აუდიტორული ორგანიზაციის დასახელება და საიდენტიფიკაციო ნომერი;
ბ) ავტორიზებული აუდიტორული ორგანიზაციის საკონტაქტო ინფორმაცია;
გ) ავტორიზებულ აუდიტორულ ორგანიზაციაში დასაქმებული ავტორიზებელი აუდიტორების სახელი და გვარი, ასევე ინფორმაციული უსაფრთხოების სფეროში მუშაობის გამოცდილება.

მუხლი 12. ავტორიზაციის საფასური

1. ავტორიზაციისთვის დაწესებული საფასური (შემდგომში – საფასური) არის სააგენტოს მიერ ავტორიზაციისთვის დადგენილი სავალდებულო გადასახდელი.
2. საფასურის გადახდა ხორციელდება აპლიკანტი ორგანიზაციის მიერ სააგენტოში განაცხადის შეტანისას.
3. სააგენტოს განაცხადთან და დოკუმენტებთან ერთად აპლიკანტი ორგანიზაციის მიერ წარედგინება გადახდის დამადასტურებელი ქვითარი. ქვითრის წარუდგენლობა წარმოადგენს განაცხადის განუხილველად დატოვების საფუძველს.
4. აპლიკანტი ორგანიზაციისთვის ავტორიზაციაზე უარის შემთხვევაში, ავტორიზაციის საფასური არ ექვემდებარება უკან დაბრუნებას.
5. ავტორიზაციის საფასური განისაზღვრება 500 (ხუთასი) ლარის ოდენობით.

დანართი 1

განაცხადი ავტორიზაციის გავლის შესახებ

შევსების თარიღი:

აპლიკანტი ორგანიზაციის დასახელება		
აპლიკანტი ორგანიზაციის საიდენტიფიკაციო ნომერი		
აპლიკანტი ორგანიზაციის მისამართი		
აპლიკანტი ორგანიზაციის მიერ უფლებამოსილი პირის საკონტაქტო ინფორმაცია	ელ.ფოსტა სახელი და გვარი	საკონტაქტო ტელეფონის ნომერი
აუდიტორის სახელი, გვარი (თუ არარეზიდენტია, სრული სახელი და გვარი)		
პირადი ნომერი		
მოქალაქეობა		
ფაქტობრივი მისამართი		
საკონტაქტო ინფორმაცია	ელ.ფოსტა	საკონტაქტო ტელეფონის ნომერი
აუდიტორი თანახმაა განთავსდეს კატალოგში მის შესახებ ინფორმაცია? *თანხმობის შემთხვევაში შეავსეთ გვერდით გრაფა.*	ხელმოწერა	

აპლიკანტი ორგანიზაცია თანახმაა განთავსდეს კატალოგში მის შესახებ ინფორმაცია? *თანხმობის შემთხვევაში შეავსეთ გვერდით გრაფები.*	ხელმოწერა	ბეჭედი

უფლებამოსილი წარმომადგენლის ხელმოწერა

ბეჭედი.