ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №8

2021 წლის 14 დეკემბერი

ქ. თბილისი

კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესისა და ავტორიზაციის პროცედურების დადგენის შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-6^1 მუხლის პირველი პუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის, „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის 25-ე მუხლისა და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ 2021 წლის 10 ივნისის №632-IVმს-Xმპ საქართველოს კანონის მე-2 მუხლის მე-2 პუნქტის „თ“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

1. დამტკიცდეს „კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესი და ავტორიზაციის პროცედურები“.
2. ძალადაკარგულად გამოცხადდეს „ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესის, ავტორიზაციის პროცედურების და ავტორიზაციის საფასურის დამტკიცების შესახებ” ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №5 ბრძანება.
3. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის
სააგენტოს თავმჯდომარე — დავით ნადირაშვილი

კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესი და ავტორიზაციის პროცედურები

თავი I. ზოგადი დებულებები

მუხლი 1. ინფორმაციული უსაფრთხოების აუდიტის და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების ავტორიზაციის მიზანი

ამ წესის მიხედვით ორგანიზაციათა ავტორიზაცია მიზნად ისახავს კრიტიკული ინფორმაციული სისტემის სუბიექტის (შემდგომ – სუბიექტი) ინფორმაციული უსაფრთხოების აუდიტისა და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის შესაბამისი კვალიფიკაციის მქონე ორგანიზაციის მიერ ჩატარებას.

მუხლი 2. მოქმედების სფერო

1. ეს წესი, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის (შემდგომ – კანონი)

შესაბამისად, განსაზღვრავს ინფორმაციული უსაფრთხოების აუდიტისა და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩასატარებლად ორგანიზაციათა ავტორიზაციის წესს და ადგენს:

ა) ავტორიზაციის შესახებ განცხადების ფორმასა და მისი წარდგენის წესს;

ბ) ავტორიზაციის შესახებ განცხადებისა და წარმოდგენილი დოკუმენტაციის განხილვის წესსა და ვადებს;

გ) ავტორიზაციის გავლის ან მასზე უარის თქმის საფუძვლებსა და შესაბამის ვადებს;

დ) ავტორიზებული ორგანიზაციების აღრიცხვის ფორმას;

ე) ავტორიზაციის გაუქმების საფუძვლებს.

2. ორგანიზაციათა ავტორიზაციასთან დაკავშირებით გადაწყვეტილებას იღებს საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი – ციფრული მმართველობის სააგენტოს (შემდგომ – სააგენტო).

მუხლი 3. ტერმინთა განმარტება

ამ წესში გამოყენებულ ტერმინებს აქვთ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით განსაზღვრული მნიშვნელობა.

თავი II. ავტორიზაცია

მუხლი 4. ინფორმაციული უსაფრთხოების აუდიტის და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების ავტორიზაციის შინაარსი

1. ინფორმაციული უსაფრთხოების აუდიტისა და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების ავტორიზაცია წარმოადგენს სააგენტოს მომსახურებას, რომლის გაწევაც იწყება განცხადების რეგისტრაციის მომენტიდან.

2. ამ წესის მე-2 მუხლით განსაზღვრული ავტორიზაცია მოიცავს შემდეგ ეტაპებს:

ა) ინფორმაციული უსაფრთხოების აუდიტისა ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის განხორციელების მსურველი ორგანიზაციის (შემდგომ – განმცხადებელი) ამ წესით დადგენილ მოთხოვნებთან შესაბამისობის შემოწმებას, რაც გულისხმობს ორგანიზაციაში დასაქმებული აუდიტორ(ებ)ის ან/და შეღწევადობის (პენეტრაციის) ტესტის განმახორციელებელი პირების (შემდგომ ტესტის განმახორციელებელი პირები) ცოდნისა და კვალიფიკაციის შემოწმებას;

ბ) საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით განსაზღვრულ უსაფრთხოების მოთხოვნებთან ორგანიზაციის შესაბამისობის შემოწმებას (გარდა მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის/შეღწევადობის (პენეტრაციის) ტესტის განმახორციელებელი ორგანიზაციებისა);

გ) საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით განსაზღვრული წესის შესაბამისად ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარების უფლებამოსილების მქონე თანამშრომლის უსაფრთხოებაზე შემოწმებას (გარდა მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკების აუდიტორებისა/ტესტის განმახორციელებელი პირებისა).

3. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკში ინფორმაციული უსაფრთხოების აუდიტი ან/და პენეტრაციის ტესტი კომერციული ბანკის შერჩევით შეიძლება ჩაატარონ აგრეთვე კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და

პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებულმა ორგანიზაციებმა, რომელთა სიას კომერციული ბანკების მოთხოვნის საფუძველზე სააგენტოს წარუდგენს საქართველოს ეროვნული ბანკი. სააგენტო, ამ წესის შესაბამისად, უზრუნველყოფს აღნიშნული ორგანიზაციების ავტორიზაციას კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებული ორგანიზაციების დამატებით სიაში რეგისტრაციით.

მუხლი 5. ავტორიზებული ორგანიზაციები

1. ავტორიზაციის გავლის უფლება აქვს როგორც საქართველოში, ასევე – საზღვარგარეთ რეგისტრირებულ იურიდიულ პირს/მის ფილიალს. დაუშვებელია ავტორიზაციის გაცემა, თუ იურიდიული პირის საქმიანობიდან, მიზნებიდან ან/და რეპუტაციიდან გამომდინარე, არსებობს ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარების პროცესში ან მის შემდგომ სუბიექტის ინფორმაციული სისტემის შეფერხების ან მწყობრიდან გამოსვლის სავარაუდო საფრთხე.

2. ინფორმაციული უსაფრთხოების აუდიტისა და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარებაზე უფლებამოსილ პირებს წარმოადგენენ ავტორიზებული ორგანიზაციის ის თანამშრომლები (აუდიტორები, ტესტის განმახორციელებელი პირები), რომლებიც მითითებულნი იქნებიან ავტორიზაციის მინიჭების შესახებ გადაწყვეტილებაში.

მუხლი 6. ავტორიზაციის შესახებ განცხადება

1. განმცხადებელი მისი უფლებამოსილი წარმომადგენლის მეშვეობით ავსებს ამ წესის №1ა/№1ბ დანართით განსაზღვრულ შესაბამისი განცხადების ფორმას, ხოლო ინფორმაციული უსაფრთხოების აუდიტორი/ტესტის გამარხორციელებელი პირი ავსებს ამ წესის №2 დანართით განსაზღვრულ შესაბამისი განცხადების ფორმას, სადაც მიეთითება მხოლოდ ერთი ინფორმაციული უსაფრთხოების აუდიტორი/ტესტის განმახორციელებელი პირი.

2. განცხადებასთან ერთად განმცხადებელი სააგენტოში ასევე წარადგენს:

ა) ინფორმაციული უსაფრთხოების აუდიტორის/ტესტის განმახორციელებელი პირის რეზიუმეს;

ბ) ორგანიზაციაში დასაქმებული ინფორმაციული უსაფრთხოების აუდიტორის/ტესტის განმახორციელებელი პირის კომპეტენციის დამადასტურებელი დოკუმენტ(ებ)ის ასლ(ებ)ი. ამასთანავე:

ბ.ა) სავალდებულოა ასლის დედანთან სისწორე დამოწმებული იყოს სანოტარო წესით, თუ წარმოდგენილია ამ წესის მე-9 მუხლის პირველი პუნქტით გათვალისწინებული რომელიმე სერტიფიკატი, რომლის ვალიდურობაც არ არის გადამოწმებადი შემდეგ ვებსაიტზე: Credly (https://www.credly.com);

ბ.ბ) თუ წარმოდგენილია ამ წესის მე-10 მუხლის პირველი პუნქტის „ი“ ქვეპუნქტით გათვალისწინებული ერთ-ერთი სერტიფიკატის ასლი, სავალდებულოა სააგენტოს აგრეთვე წარედგინოს აღნიშნული სერტიფიკატის ორიგინალი (ელექტრონული) ეგზემპლარი, რომელზეც შესრულებულია Council of Registered Ethical Security Testers (CREST)-ის ელექტრონული ხელმოწერა/ელექტრონული შტამპი;

გ) ორგანიზაციაში დასაქმებული ინფორმაციული უსაფრთხოების აუდიტორის/ტესტის განმახორციელებელი პირის წერილობით განცხადებას (დანართი №2) ინფორმაციული უსაფრთხოების აუდიტის/შეღწევადობის (პენეტრაციის) ტესტის ჩატარებისას დამოუკიდებლობის, კონფიდენციალურობის, ობიექტურობის და მიუკერძოებლობის პრინციპების დაცვის თაობაზე;

დ) „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 გათვალისწინებული საფასურის გადახდის დამადასტურებელ დოკუმენტს.

3. (ამოღებულია - 10.06.2024, №2).

4. განცხადება და თანდართული დოკუმენტები შედგენილი უნდა იყოს ქართულ ენაზე, ხოლო უცხო ენაზე შედგენილ დოკუმენტს უნდა ერთოდეს სანოტარო წესით დამოწმებული თარგმანი ქართულ ენაზე.
ციფრული მმართველობის სააგენტოს თავმჯდომარის 2024 წლის 10 ივნისის ბრძანება №2 - ვებგვერდი, 12.06.2024წ.

მუხლი 7. ავტორიზაციის საფასური

1. ავტორიზაციისთვის დაწესებული საფასური (შემდგომ – საფასური) არის სავალდებულო გადასახდელი, რომელიც განსაზღვრულია „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.

2. საფასურის გადახდა ხორციელდება განმცხადებლის მიერ სააგენტოში განცხადების შეტანისას. საფასური გადაიხდება ერთეულ განცხადებაზე.

3. ავტორიზაციაზე უარის ან მისი განუხილველად დატოვების შემთხვევაში, ავტორიზაციის საფასური არ ექვემდებარება უკან დაბრუნებას.

მუხლი 8. ავტორიზაციის შესახებ განცხადების განხილვა

1. სააგენტო ამოწმებს შემოსული განცხადებისა და მასზე თანდართული დოკუმენტების შესაბამისობას ამ წესის მოთხოვნებთან. თუ წარმოდგენილი განცხადება და მასზე თანდართული დოკუმენტები არასრული ან არაზუსტია, სააგენტო 10 დღის ვადაში ატყობინებს განმცხადებელს აღნიშნულის შესახებ წერილობით და დამატებითი დოკუმენტის ან/და ინფორმაციის წარსადგენად განუსაზღვრავს დამატებით ვადას, რომელიც არ შეიძლება იყოს 5 დღეზე ნაკლები. აღნიშნული ვადა განმცხადებლის მოთხოვნით სააგენტომ შესაძლოა გააგრძელოს მხოლოდ ერთხელ, მაგრამ არაუმეტეს 15 დღის ვადით. დამატებითი დოკუმენტის ან სხვა ინფორმაციის წარდგენამდე განცხადების განხილვის ვადის დინება შეჩერებულად ითვლება. განცხადების განხილვის ვადის დინება განახლდება შესაბამისი დოკუმენტის ან/და ინფორმაციის წარდგენისთანავე.

2. სააგენტო უფლებამოსილია, განმცხადებელს მოსთხოვოს დამატებითი ინფორმაციის წარდგენა ან/და წარდგენილი ინფორმაციის დაზუსტება.

3. ამ წესის მე-12 მუხლით გათვალისწინებულ შემთხვევებში, სააგენტო მიმართავს შესაბამის სახელმწიფო ორგანოს ავტორიზაციის მინიჭების მიზანშეწონილობის თაობაზე გადაწყვეტილების მიღების მოთხოვნით. გადაწყვეტილების მიღებამდე განცხადების განხილვის ვადის დინება შეჩერებულად ითვლება. განცხადების განხილვის ვადის დინება განახლდება შესაბამისი ინფორმაციის მიღებისთანავე.

4. სააგენტო გადაწყვეტილებას იღებს დოკუმენტაციის სრულად წარდგენიდან 90 კალენდარული დღის განმავლობაში.

5. სააგენტო, ამ წესის მე-6 მუხლით გათვალისწინებული დოკუმენტაციის შემოწმების შედეგად და ამ წესის მე-12 მუხლით გათვალისწინებულ შემთხვევებში, უფლებამოსილი ორგანოსგან მიღებული ინფორმაციის გათვალისწინებით, იღებს ერთ-ერთ შემდეგ გადაწყვეტილებას:

ა) ავტორიზაციის შესახებ განცხადების სრულად დაკმაყოფილების თაობაზე;

ბ) ავტორიზაციის შესახებ განცხადების დაკმაყოფილებაზე უარის თქმის თაობაზე;

გ) ავტორიზაციის შესახებ განცხადების განუხილველად დატოვების თაობაზე.

6. სააგენტოს გადაწყვეტილება მისი მიღებიდან 5 დღის განმავლობაში გადაეცემა ან ფოსტის/ელექტრონული ფოსტის მეშვეობით ეგზავნება განმცხადებელს.

7. ავტორიზაციისას უზრუნველყოფილი უნდა იყოს დამოუკიდებლობის, კონფიდენციალურობის, ობიექტურობის და მიუკერძოებლობის პრინციპების დაცვა.

8. აუდიტის განმახორციელებელ ორგანიზაციას ან/და აუდიტორს ეკრძალება სუბიექტში ინფორმაციული უსაფრთხოების აუდიტის ჩატარება, თუ მას ამ სუბიექტში დანერგილი აქვს ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს). აღნიშნული შეზღუდვა მოქმედებს, ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) დანერგვიდან 3 წლის განმავლობაში.

9. სააგენტოს მიერ მიღებული გადაწყვეტილება შესაძლოა გასაჩივრდეს სასამართლოში საქართველოს კანონმდებლობით დადგენილი წესითა და პირობებით.

მუხლი 9. მოთხოვნები ინფორმაციული უსაფრთხოების აუდიტის განხორციელების მსურველი ორგანიზაციის მიმართ

1. განცხადებაში მითითებულ, განმცხადებელთან დასაქმებულ აუდიტორ(ებ)ს უნდა ჰქონდეს ინფორმაციული უსაფრთხოების აუდიტის მიმართულებით კომპეტენციის დამადასტურებელი ერთ-ერთი შემდეგი მოქმედი სერტიფიკატი: ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) აუდიტორის/წამყვანი აუდიტორის სერტიფიკატი (ISMS Auditor/Lead Auditor Certificate), რომელიც აღიარებულია სერტიფიცირებული აუდიტორების საერთაშორისო რეესტრის (The International Register of Certificated Auditors (IRCA)) მიერ ან ინფორმაციული სისტემების აუდიტისა კონტროლის ასოციაციის (Information Systems Audit and Control Association) მიერ გაცემული CISA სერტიფიკატი. განცხადების წარმოდგენის მომენტისთვის აღნიშნული სერტიფიკატის ვადის გასვლამდე დარჩენილი უნდა იყოს არანაკლებ 6 თვისა.

2. (ამოღებულია - 10.06.2024, №2).

ციფრული მმართველობის სააგენტოს თავმჯდომარის 2022 წლის 5 აგვისტოს ბრძანება №1 - ვებგვერდი, 08.08.2022წ.
ციფრული მმართველობის სააგენტოს თავმჯდომარის 2024 წლის 10 ივნისის ბრძანება №2 - ვებგვერდი, 12.06.2024წ.

მუხლი 10. მოთხოვნები ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის განხორციელების მსურველი ორგანიზაციის მიმართ

1. განცხადებაში მითითებულ, განმცხადებელთან დასაქმებულ ტესტის განმახორციელებელ პირს უნდა ჰქონდეს ქვემოთ მოცემული ერთ-ერთი ორგანიზაციის მიერ გაცემული კომპეტენციის დამადასტურებელი ერთ-ერთი მოქმედი სერტიფიკატი:

ა) ორგანიზაცია: Offensive Security (OffSec). სერტიფიკატი:

ა.ა) OffSec Certified Professional (OSCP);

ა.ბ) OffSec Certified Expert (OSCE);

ა.გ) OffSec Web Expert (OSWE);

ა.დ) OffSec Exploitation Expert (OSEE);

ა.ე) OffSec Experienced Pentester (OSEP);

ა.ვ) OffSec Exploit Developer (OSED);

ბ) ორგანიზაცია: International Council of E-Commerce Consultants (EC-Council). სერტიფიკატი:

ბ.ა) Certified Ethical Hacker (CEH);

ბ.ბ) Certified Penetration Testing Professional (CPENT);

ბ.გ) Licensed Penetration Tester (LPT);

გ) ორგანიზაცია: The Computing Technology Industry Association (CompTIA). სერტიფიკატი: PenTest+;

დ) ორგანიზაცია: The Global Information Assurance Certification (GIAC). სერტიფიკატი:

დ.ა) GIAC Penetration Tester (GPEN);

დ.ბ) GIAC Web Application Penetration Tester (GWAPT);

დ.გ) GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);

დ.დ) GIAC Certified Incident Handler (GCIH);

ე) ორგანიზაცია: INE Security. სერტიფიკატი:

ე.ა) eLearnSecurity Junior Penetration Tester (eJPT);

ე.ბ) eLearnSecurity Certified Professional Penetration Tester (eCPPT);

ე.გ) eLearnSecurity Web Application Penetration Tester (eWPT);

ე.დ) eLearnSecurity Web application Penetration Tester eXtreme (eWPTX);

ვ) ორგანიზაცია: Hack The Box Ltd (HackTheBox). სერტიფიკატი:

ვ.ა) Certified Penetration Testing Specialist (HTB CPTS);

ვ.ბ) Certified Web Exploitation Expert (HTB CWEE);

ზ) ორგანიზაცია: Zero-Point Security. სერტიფიკატი:

ზ.ა) Certified Red Team Operator (CRTO);

ზ.ბ) Certified Red Team Lead (CRTL);

თ) ორგანიზაცია: Altered Security. სერტიფიკატი:

თ.ა) Certified Red Team Professional (CRTP);

თ.ბ) Certified Red Team Expret (CRTE);

თ.გ) Certified Red Team Master (CRTM);

ი) ორგანიზაცია: Council of Registered Ethical Security Testers (CREST). სერტიფიკატი:

ი.ა) CREST Certified Tester - Infrastructure (CCT INF);

ი.ბ) CREST Certified Tester - Application (CCT APP);

ი.გ) CREST Certified Simulated Attack Specialist (CCSAS).

2. ამ მუხლის პირველი პუნქტის „ა“–„თ“ ქვეპუნქტებით გათვალისწინებული შესაბამისი სერტიფიკატის ვალიდურობა გადამოწმებადი უნდა იყოს ერთ-ერთ შემდეგ ვებსაიტზე: Credly (https://www.credly.com), Accredible (https://www.credential.net), ASPEN (https://aspen.eccouncil.org), INE (https://certs.ine.com), HackTheBox (https://www.hackthebox.com), Canvas Badges (https://eu.badgr.com). ამ მუხლის პირველი პუნქტის „ი“ ქვეპუნქტით გათვალისწინებული შესაბამისი სერტიფიკატის ვალიდურობა მოწმდება ამ წესის მე-6 მუხლის მე-2 პუნქტის „ბ.ბ“ ქვეპუნქტის შესაბამისად.

ციფრული მმართველობის სააგენტოს თავმჯდომარის 2022 წლის 5 აგვისტოს ბრძანება №1 - ვებგვერდი, 08.08.2022წ.
ციფრული მმართველობის სააგენტოს თავმჯდომარის 2024 წლის 10 ივნისის ბრძანება №2 - ვებგვერდი, 12.06.2024წ.

მუხლი 11. მოთხოვნები მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის/შეღწევადობის (პენეტრაციის) ტესტის განმახორციელებელი ორგანიზაციების მიმართ

1. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკში ინფორმაციული უსაფრთხოების აუდიტი ან/და პენეტრაციის ტესტი კომერციული ბანკის შერჩევით შეიძლება ჩაატარონ აგრეთვე კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებულმა ორგანიზაციებმა, რომელთა სიას კომერციული ბანკების მოთხოვნის საფუძველზე სააგენტოს წარუდგენს საქართველოს ეროვნული ბანკი ამ წესის მე-6 მუხლით განსაზღვრული წესით.

2. ციფრული მმართველობის სააგენტო ინფორმაციის მიღებიდან 10 დღის ვადაში უზრუნველყოფს ამ წესის მე-6 მუხლის მე-2 პუნქტის შესაბამისად წარმოდგენილი განცხადებისა და სხვა დოკუმენტაციის განხილვას ამ წესის მე-8 მუხლით განსაზღვრული წესით.

3. ამ მუხლით გათვალისწინებულ შემთხვევებში ორგანიზაციისთვის ავტორიზაციის მინიჭების პროცესი არ საჭიროებს ამ წესის მე-12 მუხლის მიხედვით ორგანიზაციის და მისი თანამშრომლის უსაფრთხოებაზე შემოწმებას.
ციფრული მმართველობის სააგენტოს თავმჯდომარის 2023 წლის 11 სექტემბრის ბრძანება №1 - ვებგვერდი, 12.09.2023 წ.

მუხლი 12. უსაფრთხოებაზე შემოწმება

1. ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის განმცხადებელი (გარდა მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის/შეღწევადობის (პენეტრაციის) ტესტის განმახორციელებელი ორგანიზაციებისა) უნდა აკმაყოფილებდეს საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით განსაზღვრულ უსაფრთხოების მოთხოვნებს, ხოლო მისი ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარების უფლებამოსილების მქონე თანამშრომელს, საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით დადგენილი წესის შესაბამისად, გავლილი უნდა ჰქონდეს უსაფრთხოებაზე შემოწმება.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებული, საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით განსაზღვრულ უსაფრთხოების მოთხოვნებთან შესაბამისობის თაობაზე ინფორმაციის მიღების მიზნით, სააგენტო უფლებამოსილ სახელმწიფო ორგანოს მიმართავს ამ წესის მე-8 მუხლის პირველი პუნქტის მიხედვით განცხადებისა და მასზე თანდართული დოკუმენტების ამ წესის მოთხოვნებთან შესაბამისობის დადგენიდან 5 დღის ვადაში.

3. ამ მუხლის მე-2 პუნქტით განსაზღვრული უფლებამოსილი სახელმწიფო ორგანო სააგენტოს მოთხოვნილ ინფორმაციას წარუდგენს საქართველოს სახელმწიფო უსაფრთხოების სამსახურის

უფროსის ნორმატიული აქტით დადგენილ ვადაში და წესით. უფლებამოსილი სახელმწიფო ორგანოს მიერ 60 სამუშაო დღის ვადაში სააგენტოსათვის საჭირო ინფორმაციის წარუდგენლობის შემთხვევაში, ითვლება, რომ განმცხადებელი/განცხადებაში მითითებული თანამშრომელი აკმაყოფილებს სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით განსაზღვრულ უსაფრთხოების მოთხოვნებს.

ციფრული მმართველობის სააგენტოს თავმჯდომარის 2024 წლის 10 ივნისის ბრძანება №2 - ვებგვერდი, 12.06.2024წ.

მუხლი 13. ავტორიზაციის შესახებ განცხადების სრულად დაკმაყოფილება

1. ავტორიზაციის შესახებ განცხადებისა და მასზე თანდართული დოკუმენტების/ინფორმაციის კანონთან და ამ წესთან სრულად შესაბამისობის დადგენის შემთხვევაში, სააგენტო იღებს გადაწყვეტილებას ავტორიზაციის მინიჭების შესახებ. გადაწყვეტილებაში მიეთითება ავტორიზებულ ორგანიზაციაში დასაქმებული ის აუდიტორი/ტესტის განმახორციელებელი პირი, რომლის მეშვეობითაც ავტორიზებულ ორგანიზაციას ენიჭება ინფორმაციული უსაფრთხოების აუდიტის/ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილება ამ წესის მე-9 ან მე-10 მუხლით გათვალისწინებული შესაბამისი სერტიფიკატის მოქმედების ვადის განმავლობაში, ხოლო თუ სერტიფიკატი გაცემულია განუსაზღვრელი ვადით – სააგენტოს მიერ ავტორიზაციის მინიჭების თარიღიდან სამი წლის განმავლობაში.

2. (ამოღებულია - 10.06.2024, №2).

3. ავტორიზებულ ორგანიზაციაზე გაიცემა ავტორიზაციის შესაბამისი სერტიფიკატი უნიკალური ნომრით, რომელიც დამოწმებული იქნება სააგენტოს კვალიფიციური ელექტრონული შტამპით.

4. ავტორიზაციის ვადის ათვლა იწყება სააგენტოს მიერ ამ მუხლის მე-3 პუნქტით გათვალისწინებული სერტიფიკატის გაცემის მომენტიდან.

ციფრული მმართველობის სააგენტოს თავმჯდომარის 2022 წლის 5 აგვისტოს ბრძანება №1 - ვებგვერდი, 08.08.2022წ.
ციფრული მმართველობის სააგენტოს თავმჯდომარის 2024 წლის 10 ივნისის ბრძანება №2 - ვებგვერდი, 12.06.2024წ.

მუხლი 14. ავტორიზაციაზე უარის თქმის შესახებ გადაწყვეტილება

თუ განცხადებასა და თანდართულ მასალებში მითითებული ინფორმაცია ვერ აკმაყოფილებს ავტორიზაციის მინიჭებისათვის კანონითა და ამ წესით დადგენილ მოთხოვნებს, სააგენტო იღებს გადაწყვეტილებას ავტორიზაციაზე უარის თქმის შესახებ.

მუხლი 15. ავტორიზაციის შესახებ განცხადების განუხილველად დატოვება

თუ ამ წესის მე-8 მუხლის პირველი პუნქტით დადგენილ ვადაში განმცხადებელი არ წარადგენს შესაბამის დოკუმენტს ან/და ინფორმაციას, სააგენტო გამოიტანს გადაწყვეტილებას განცხადების განუხილველად დატოვების შესახებ.

მუხლი 16. ავტორიზებული ორგანიზაციების აღრიცხვა

1. სააგენტო აღრიცხავს ავტორიზებული ორგანიზაციებისა და აუდიტორების/ტესტის განმახორციელებელი პირების სიას ამ წესის დანართი №3-ით და დანართი №4-ით დადგენილი ფორმით, რომლებიც შეიცავს შემდეგ ინფორმაციას:

ა) ავტორიზებული ორგანიზაციის დასახელებასა და საიდენტიფიკაციო ნომერს;

ბ) ავტორიზებული ორგანიზაციის საკონტაქტო ინფორმაციას;

გ) ავტორიზებულ ორგანიზაციაში დასაქმებული ავტორიზებული აუდიტორის/ტესტის განმახორციელებელი პირის სახელს, გვარს და პირად ნომერს/სხვა მაიდენტიფიცირებელ ნომერს (ასეთის არსებობის შემთხვევაში);

დ) ავტორიზაციის თარიღსა და მოქმედების ვადას;

ე) აუდიტორის/ტესტის განმახორციელებელი პირის კვალიფიკაციის დამადასტურებელი დოკუმენტის მოქმედების ვადას (ასეთის არსებობის შემთხვევაში).

2. სააგენტო კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის ხელმისაწვდომს ხდის ინფორმაციას მის მიერ ავტორიზებული ორგანიზაციებისა და აუდიტორების/ტესტის განმახორციელებელი პირების შესახებ.

3. ამ წესის მე-11 მუხლით გათვალისწინებულ შემთხვევაში, სააგენტო უზრუნველყოფს ორგანიზაციების ავტორიზაციას კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებული ორგანიზაციების დამატებით სიაში (დანართი №4) რეგისტრაციით. ამ გზით ავტორიზებული ორგანიზაციების შესახებ ინფორმაცია მიეწოდება ეროვნულ ბანკს ან/და მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკებს.

ციფრული მმართველობის სააგენტოს თავმჯდომარის 2023 წლის 11 სექტემბრის ბრძანება №1 - ვებგვერდი, 12.09.2023 წ.

თავი III. ავტორიზებული ორგანიზაციების ზედამხედველობა

მუხლი 17. ავტორიზებული ორგანიზაციების ზედამხედველობა

1. ავტორიზებული ორგანიზაცია ვალდებულია ყოველწლიურად ჩაატაროს შუალედური თვითშეფასება ავტორიზაციის მოთხოვნებთან შესაბამისობის შემოწმების მიზნით. ამ წესით დადგენილ მოთხოვნებთან მიმართებით აღმოჩენილი შეუსაბამობები მათი აღმოჩენიდან 10 დღის ვადაში უნდა ეცნობოს სააგენტოს.

2. ავტორიზაცია შეწყდება:

ა) თუ ავტორიზებული აუდიტორი/შეღწევადობის (პენეტრაციის) ტესტის ჩამტარებელი არცერთი პირი აღარ არის დასაქმებული ავტორიზებულ ორგანიზაციაში;

ბ) ავტორიზებული აუდიტორის/შეღწევადობის (პენეტრაციის) ტესტის ჩამტარებლის სერტიფიკატი ძალადაკარგულია ინფორმაციული უსაფრთხოების აუდიტის/შეღწევადობის (პენეტრაციის) ტესტის ჩატარებისას;

გ) თუ სააგენტოსთვის ცნობილი გახდა, რომ ავტორიზაციის მინიჭების მიზნით წარდგენილი დოკუმენტ(ები)ი იყო არასწორი ან შეცდომაში შემყვანი;

დ) ამ წესის მე-8 მუხლის მე-8 პუნქტით გათვალისწინებულ შემთხვევაში.

3. ავტორიზებული ორგანიზაცია, თუ მან დაკარგა ავტორიზაცია ზემოაღნიშნული საფუძვლით, იმისათვის რათა მოიპოვოს ინფორმაციული უსაფრთხოების აუდიტის/ შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლება, ვალდებულია ხელახლა გაიაროს ავტორიზაციის პროცედურა.

4. ავტორიზებული ორგანიზაციის აუდიტორის/შეღწევადობის (პენეტრაციის) ტესტის ჩამტარებლის სხვა ორგანიზაციაში გადასვლა არ იწვევს ამ უკანასკნელის მიერ ავტორიზაციის მოპოვებას. აღნიშნულმა ორგანიზაციამ უნდა გაიაროს ავტორიზაცია ამ წესის შესაბამისად.

5. სააგენტოს გადაწყვეტილებაში მითითებულ პირებს ინფორმაციული უსაფრთხოების აუდიტის/შეღწევადობის (პენეტრაციის) ტესტის ჩატარება შეუძლიათ მხოლოდ ერთი ავტორიზებული

ორგანიზაციის სახელით.

მუხლი 18. სააგენტოსთან კომუნიკაცია

1. ამ წესით გათვალისწინებული განცხადება და სხვა დოკუმენტ(ებ)ი სააგენტოს მიეწოდება წერილობითი ფორმით, მატერიალური სახით ან ელექტრონულად. ელექტრონული დოკუმენტი უნდა აკმაყოფილებდეს „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის მოთხოვნებს.

2. სააგენტო განმცხადებელს/ავტორიზებულ ორგანიზაციას ამ წესით გათვალისწინებულ დოკუმენტ(ებ)ს უგზავნის მისთვის ცნობილ მისამართზე/ელექტრონული ფოსტის მისამართზე.

დანართი №1ა

ინფორმაციული უსაფრთხოების აუდიტის განხორციელების მსურველი ორგანიზაციის განცხადება ავტორიზაციის შესახებ

შევსების თარიღი: _____

ინფორმაცია ინფორმაციული უსაფრთხოების აუდიტის განხორციელების მსურველი ორგანიზაციის შესახებ	
ორგანიზაციის დასახელება	
ორგანიზაციის საიდენტიფიკაციო ნომერი	
ორგანიზაციის მისამართი (ქვეყანა, ქალაქი, ქუჩა, ნომერი)	
ინფორმაცია ორგანიზაციის დამფუძნებლების/ პარტნიორების შესახებ	
წარმომადგენლობაზე უფლებამოსილი პირის საკონტაქტო ინფორმაცია	
სახელი, გვარი და პირადი ნომერი	
მოქალაქეობა	
ტელეფონის ნომერი	
ელ. ფოსტა	

ინფორმირებული ვარ, რომ ინფორმაციული უსაფრთხოების აუდიტისა და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების ავტორიზებული ორგანიზაციებისა და აუდიტორების/შეღწევადობის (პენეტრაციის) განმახორციელებელი პირების სიაში აღირიცხება განმცხადებლის შესახებ კანონმდებლობით განსაზღვრული ინფორმაცია და ხელმისაწვდომი გახდება შესაბამისი კრიტიკული ინფორმაციული სისტემის სუბიექტებისა და საქართველოს კანონმდებლობით განსაზღვრული სხვა დაწესებულებებისთვის.

ინფორმირებული ვარ, რომ მოქმედი კანონმდებლობის თანახმად, აუდიტის განმახორციელებელ ორგანიზაციას ან/და აუდიტორს ეკრძალება სუბიექტში ინფორმაციული უსაფრთხოების აუდიტის ჩატარება, თუ მას ამ სუბიექტში დანერგილი აქვს ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს) და რომ აღნიშნული შეზღუდვა მოქმედებს, ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) დანერგვიდან 3 წლის განმავლობაში.

უფლებამოსილი წარმომადგენლის ხელმოწერა

ბეჭედი

ციფრული მმართველობის სააგენტოს თავმჯდომარის 2023 წლის 13 სექტემბრის ბრძანება №2 - ვებგვერდი, 13.09.2023 წ.

დანართი №1ბ

ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის განხორციელების მსურველი ორგანიზაციის განცხადება ავტორიზაციის შესახებ

შევსების თარიღი: _____

ინფორმაცია ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის განხორციელების მსურველი ორგანიზაციის შესახებ	
ორგანიზაციის დასახელება	
ორგანიზაციის საიდენტიფიკაციო ნომერი	
ორგანიზაციის მისამართი (ქვეყანა, ქალაქი, ქუჩა, ნომერი)	
ინფორმაცია ორგანიზაციის დამფუძნებლების/პარტნიორების შესახებ	
წარმომადგენლობაზე უფლებამოსილი პირის საკონტაქტო ინფორმაცია	
სახელი, გვარი და პირადი ნომერი	
მოქალაქეობა	
ტელეფონის ნომერი	
ელ. ფოსტა	

ინფორმირებული ვარ, რომ ინფორმაციული უსაფრთხოების აუდიტისა და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების ავტორიზებული ორგანიზაციებისა და აუდიტორების/შეღწევადობის (პენეტრაციის) განმახორციელებელი პირების სიაში აღირიცხება განმცხადებლის შესახებ კანონმდებლობით განსაზღვრული ინფორმაცია და ხელმისაწვდომი გახდება შესაბამისი კრიტიკული ინფორმაციული სისტემის სუბიექტებისა და საქართველოს კანონმდებლობით განსაზღვრული სხვა დაწესებულებებისთვის.

უფლებამოსილი წარმომადგენლის ხელმოწერა

ბეჭედი

ციფრული მმართველობის სააგენტოს თავმჯდომარის 2023 წლის 13 სექტემბრის ბრძანება №2 - ვებგვერდი, 13.09.2023 წ.

დანართი №2

სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარეს

სახელი და გვარი[1]	
პირადი ნომერი[2]	
მოქალაქეობა	
მისამართი	
ტელეფონი	
ელ. ფოსტა	

განცხადება

წინამდებარე განცხადებაზე ხელმოწერით ვაცხადებ თანხმობას, რომ _____[3]-ისთვის ავტორიზაციის მინიჭების შემთხვევაში ავტორიზაციის ვადის განმავლობაში მისი სახელით განვახორციელო *(გთხოვთ, მონიშნოთ):*

☐ ინფორმაციული უსაფრთხოების აუდიტი;

☐ ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი.

რომლის ფარგლებშიც, ჩემს მიერ დაცული იქნება დამოუკიდებლობის, კონფიდენციალურობის, ობიექტურობის და მიუკერძოებლობის პრინციპები.

ინფორმირებული ვარ, რომ ინფორმაციული უსაფრთხოების აუდიტისა და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების ავტორიზებული ორგანიზაციებისა და აუდიტორების/შეღწევადობის (პენეტრაციის) განმახორციელებელი პირების სიაში აღირიცხება ჩემ შესახებ შემდეგი ინფორმაცია: სახელი, გვარი, პირადი ნომერი, დამსაქმებელი ორგანიზაციის დასახელება, საიდენტიფიკაციო ნომერი და კვალიფიკაციის დამადასტურებელი დოკუმენტის რეკვიზიტები და ხელმისაწვდომი გახდება შესაბამისი კრიტიკული ინფორმაციული სისტემის სუბიექტებისა და საქართველოს კანონმდებლობით განსაზღვრული სხვა დაწესებულებებისთვის.

ინფორმირებული ვარ, რომ მოქმედი კანონმდებლობის თანახმად, აუდიტის განმახორციელებელ ორგანიზაციას ან/და აუდიტორს ეკრძალება სუბიექტში ინფორმაციული უსაფრთხოების აუდიტის ჩატარება, თუ მას ამ სუბიექტში დანერგილი აქვს ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს) და რომ აღნიშნული შეზღუდვა მოქმედებს, ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) დანერგვიდან 3 წლის განმავლობაში.

---

[1] არარეზიდენტის შემთხვევაში სრული სახელი და გვარი

[2] არარეზიდენტის შემთხვევაში ალტერნატიულად შესაძლებელია სხვა მაიდენტიფიცირებელი მონაცემის მითითება. მაგ.: პასპორტის ნომერი.

[3] ორგანიზაციის დასახელება და საიდენტიფიკაციო ნომერი

თარიღი:

ხელმოწერა:

ციფრული მმართველობის სააგენტოს თავმჯდომარის 2023 წლის 13 სექტემბრის ბრძანება №2 - ვებგვერდი, 13.09.2023 წ.

დანართი №3

ავტორიზებული ორგანიზაციებისა და აუდიტორების/შეღწევადობის (პენეტრაციის) განმახორციელებელი პირების სია

№	ორგანიზაციის დასახელება	აუდიტორის სახელი, გვარი და პირადი ნომერი	აკრედიტაციის/ სერტიფიკატის გამცემი ორგანოს დასახელება	სერტიფიკატის მოქმედების ვადა	ორგანიზაციის საიდენტიფიკაციო ნომერი	ავტორიზაციის ტიპი				შენიშვნა
						ინფორმაციული უსაფრთხოება	ავტორიზაციის თარიღი	შეღწევადობა	ავტორიზაციის თარიღი	
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

დანართი №4

ავტორიზებული ორგანიზაციებისა და აუდიტორების/შეღწევადობის (პენეტრაციის) განმახორციელებელი პირების დამატებითი სია – კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებული ორგანიზაციები

№	ორგანიზა-ციის დასახელება	აუდიტორის სახელი, გვარი და პირადი ნომერი	აკრედიტაციის/ სერტიფიკა-ტის გამცემი ორგანოს დასახელება	სერტიფიკა-ტის მოქმედების ვადა	ორგანიზა-ციის საიდენტიფი-კაციო ნომერი	ავტორიზაციის ტიპი				შენიშვნა
						ინფორმა-ციული უსაფრთხო-ება	ავტორიზა-ციის თარიღი	შეღწევა-დობა	ავტორიზაციის თარიღი	
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										